SpeedStream®

# Roteador
# Guia do usuário

**Modelos 4100 e 4200**

Nº de peça 007-4037-001

**© Copyright 2004, Siemens Subscriber Network.**
**Todos os direitos reservados. Impresso nos EUA.**

Os nomes dos produtos aqui mencionados podem ser marcas comerciais e/ou marcas registradas de suas respectivas empresas. A Siemens Subscriber Networks não será responsável por erros técnicos, erros editoriais ou omissões neste documento, nem por danos incidentais ou conseqüenciais resultantes do fornecimento, desempenho ou uso deste material.

## Siemens Subscriber Networks – Licença de Software e Garantia Limitada para o Usuário

A INSTALAÇÃO DO HARDWARE E DO SOFTWARE FORNECIDOS PELA SIEMENS SUBSCRIBER NETWORKS (SSN) CONSTITUI-SE NA ACEITAÇÃO DOS TERMOS DO CONTRATO DE LICENÇA DE SOFTWARE E DA GARANTIA LIMITADA A SEGUIR. CASO VOCÊ NÃO ACEITE ESTAS CONDIÇÕES, DEVOLVA O HARDWARE E SOFTWARE COM EMBALAGEM ORIGINAL À LOJA OU OUTRO FORNECEDOR DE QUEM VOCÊ ADQUIRIU O PRODUTO PARA UM REEMBOLSO TOTAL DA QUANTIA PAGA .

Os parágrafos a seguir descrevem sua licença de uso do software (“Software"), que foi fornecido com o equipamento SSN DSL a ser instalado nas dependências do cliente (“Hardware”) e a garantia limitada fornecida pela SSN ao software e hardware.

**Licença de software**

O Software é protegido por leis e tratados de direitos autorais internacionais. O Software é licenciado e não pode ser vendido ao usuário. Portanto, embora o usuário seja proprietário dos meios (CD-ROM ou disquete) nos quais o Software esteja armazenado, a SSN deterá os direitos sobre o Software.

1. **Concessão da licença** O usuário pode instalar e utilizar uma (e apenas uma) cópia do Software no computador no qual o Hardware está instalado. Se o Hardware for instalado em uma rede, o usuário pode instalar o Software no servidor de rede ou outro dispositivo localizado no servidor no qual o Hardware está sendo instalado e nos dispositivos localizados no cliente conectados à rede, se necessário.

2. **Restrições** A licença concedida é uma licença limitada. O usuário NÃO poderá: sublicenciar, transferir ou distribuir cópias do Software a terceiros; descompilar, alterar por meio de engenharia reversa, desmontar ou de outra forma reduzir o Software ou parte deste a uma forma perceptível; modificar, adaptar, traduzir ou criar trabalhos derivados com base no Software ou parte deste; alugar, locar, emprestar ou de outra forma obter lucro com o Software.

3. **Transferência** O usuário somente poderá transferir o Software se o Hardware também for transferido. Em tais casos, o usuário deve remover todas as cópias do Software de qualquer dispositivo no qual este foi instalado e certificar-se de que a parte à qual o Hardware foi transferido receba este contrato de licença e garantia limitada.

4. **Atualizações** Esta licença cobre o Software originalmente fornecido ao usuário junto com o Hardware e qualquer software adicional que venha a ser recebido da SSN, seja este transmitido por meios tangíveis (CD-ROM ou disquete), transferido da SSN ou enviado por meio de suporte do cliente. Qualquer software adicional será considerado “Software” para todos os fins desta licença.

5. **Leis e garantias de exportação** O usuário reconhece que o Software pode estar sujeito a leis e regulamentos de controle de exportação dos Estados Unidos. O usuário garante que não exportará ou re-exportará o Software a quaisquer países sujeitos a restrições de exportação.

6. **Direitos de concessão** Com exceção da licença limitada concedida expressamente neste documento, nenhuma outra licença, quer seja expressa ou implícita, por decadência ou outro motivo, será concedida a quaisquer direitos autorais, patentes, marcas registradas, segredos industriais ou outros direitos proprietário da SSN.

7. **Revogação** Sem limitação a outros direitos da SSN, a SSN poderá revogar esta licença caso o usuário deixe de cumprir qualquer uma destas cláusulas. No caso de revogação, o usuário deve destruir o Software e todas as cópias deste.

**Garantia limitada**

As seguintes garantias limitadas fornecidas pela SSN são concedidas ao usuário original do Hardware/licenciado do Software e não são atribuíveis ou transferíveis a qualquer outro comprador/licenciado.

1. **Hardware** A SSN garante que o Hardware será fornecido livre de defeitos no material ou no acabamento e funcionará essencialmente de acordo com a documentação do usuário relativa ao Hardware pelo período de um ano a contar da data de seu recebimento pelo usuário original.

2. **Software** A SSN garante que o Software funcionará essencialmente de acordo com a documentação do usuário final fornecida com o Hardware e o Software por um período de noventa dias a contar da data na qual o usuário final recebeu o Hardware e o Software. O usuário final é responsável pela seleção de hardware e software usados em seus sistemas. Dada à grande variedade de hardware e aplicativos de terceiros, a SSN não garante a compatibilidade ou a operação contínua ou livre de falhas de nosso Software com o sistema do usuário final.

3. **Direitos exclusivos** Em caso de violação desta garantia limitada, o usuário terá direito de receber da SSN, a critério exclusivo da SSN, (a) um reembolso do valor de compra pago pelo Hardware/Software ou (b) o reparo ou a substituição do Hardware/Software por produtos novos ou remanufaturados. Qualquer Hardware ou Software de reposição será garantido pelo prazo restante do período de garantia original ou por 30 (trinta) dias, o que for maior.

4. **Procedimentos de garantia** Na ocorrência de um problema durante o período da garantia limitada, o usuário final deverá seguir o procedimento descrito abaixo:

A. Antes da devolução do produto sob garantia, o usuário final deverá entrar em contato com a SSN pelo telefone (888) 286-9375 (EUA), ou enviar um e-mail para o suporte da SSN no endereço support.ssn@siemens.com para obter um número de autorização de devolução de materiais (RMA). Os RMAs são emitidos entre 8 e 17h. horário central dos EUA, exceto nos fins de semana e feriados. O usuário final deve fornecer o(s) número(s) de série do(s) produto(s) para obter um RMA.

B. Após receber um RMA, o usuário final deverá enviar o produto, incluindo fonte(s) de alimentação e cabo, quando aplicável, com frete ou postagem pré-paga e com seguro, para a SSN no endereço 4849 Alpha Road, Dallas, Texas 75244, EUA. No prazo de cinco (5) dias da notificação da SSN, o usuário final deverá fornecer à SSN quaisquer itens ausentes ou, a critério exclusivo da SSN, a SSN poderá (a) substituir os itens ausentes e cobrar do usuário final ou (b) devolver o produto ao usuário final, que arcará com as despesas de frete. O usuário final deverá informar um endereço de resposta e um número de telefone e/ou fax para contato em horário comercial. O número do RMA deve estar claramente impresso na parte externa da embalagem.

C. Os produtos devolvidos serão testados no recebimento pela SSN. Os produtos aprovados em todos os testes funcionais serão devolvidos ao usuário final.

D. A SSN devolverá o produto reparado ou substituído ao usuário final no endereço fornecido pelo mesmo por conta da SSN. Para produtos transportados dentro dos Estados Unidos, a SSN empreenderá os esforços possíveis para assegurar a remessa dentro de cinco (5) dias úteis da data de recebimento pela SSN. O serviço expresso está disponível, com custo adicional por conta do usuário final.

E. A pedido da SSN, o usuário final deve comprovar a data original da compra do produto por meio de nota fiscal de venda ou recibo detalhado com data.

5. **Limitações**

O usuário final não terá direito à cobertura ou benefício desta garantia limitada se o produto for submetido ao uso incorreto, condições anormais, armazenamento inadequado, exposição a umidade, modificações não autorizadas, reparo não autorizado, uso impróprio, negligência, maltrato, acidente, transformação, instalação inadequada ou outros atos que não sejam por culpa da SSN, inclusive atos da natureza e danos causados pelo transporte.

A SSN não será responsável e revogará a garantia se: (1) o selo ou número de série no produto tiver sido alterado indevidamente, (2) o estojo do produto tiver sido aberto ou (3) tiver ocorrido qualquer tentativa de reparo ou reparo ou modificação do produto por qualquer pessoa que não seja um prestador de serviço autorizado pela SSN.

A garantia limitada não abrange defeitos na aparência, aspecto físico, decorativo ou estrutural, inclusive construção, e quaisquer partes não operantes.

O limite da responsabilidade da SSN sob a garantia limitada será o valor real em dinheiro do produto no momento em que o usuário final devolver o produto para reparo, determinado pelo preço pago pelo usuário final no produto menos um desconto razoável pelo uso. A SSN não se responsabilizará por quaisquer outras perdas ou danos.

O usuário final será responsável por quaisquer peças ou encargos de mão-de-obra não cobertos por esta garantia limitada. O usuário final será responsável por quaisquer despesas relacionadas à reinstalação do produto.

ESTA GARANTIA LIMITADA É A ÚNICA GARANTIA FORNECIDA PELA SSN AO PRODUTO E O SOFTWARE. DENTRO DOS LIMITES PERMITIDOS PELA LEI, NENHUMA OUTRA GARANTIA SERÁ CONCEDIDA, SEJA EXPRESSA, IMPLÍCITA OU PREVISTA POR LEI, INCLUINDO QUALQUER GARANTIA DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM FIM ESPECÍFICO.

6. **Reparo fora da garantia** O conserto fora da garantia está disponível por meio de valores fixos. Entre em contato com a SSN nos números fornecidos acima para determinar a cotação do conserto feito fora da garantia. Usuários finais que procuram conserto fora da garantia devem contatar a SSN conforme descrito acima para obter um RMA e determinar o pagamento do custo do reparo. Todos os custos de remessa ficarão a cargo do usuário final.

**Cláusulas gerais**

As cláusulas gerais a seguir aplicam-se à licença de software e garantia limitada precedentes.

1. **Exclusão de garantias** A garantia limitada precedente é a única garantia expressa concedida ao usuário final, que é fornecida em lugar de quaisquer outras garantias, expressas ou implícitas. Nenhuma informação oral ou escrita ou aviso fornecido pela SSN ou seus fornecedores, distribuidores, empregados ou agentes poderá de forma alguma ampliar, modificar ou ser adicionada à licença de software e garantia limitada. Esta licença de software e garantia limitada constitui o contrato integral entre a SSN e o usuário final e substitui todos os contratos, acordos ou representações anteriores e contemporâneas, verbais ou escritos. Esta licença de software e garantia limitada não devem ser modificadas ou alteradas, exceto por documento por escrito assinado por um funcionário devidamente autorizado pela SSN.

A SSN não se responsabiliza nem autoriza qualquer centro de serviço autorizado ou qualquer outra pessoa ou entidade a assumir quaisquer outras obrigações ou responsabilidades além daquelas explicitamente determinadas nesta garantia limitada, incluindo o fornecedor ou vendedor de qualquer extensão de garantia ou contrato de serviço.

O período da garantia limitada dos anexos e acessórios fornecidos pela SSN é definido especificamente em seus próprios cartões de garantia e embalagens.

2. **EXCLUSÃO POR PREJUÍZOS INCIDENTAIS, CONSEQÜENCIAIS E OUTROS PREJUÍZOS** ATÉ AO LIMITE MÁXIMO PERMITIDO PELA LEI APLICÁVEL, EM NENHUMA HIPÓTESE A SSN SERÁ RESPONSÁVEL, SEJA POR MEIO DE CONTRATO, GARANTIA, ATO ILÍCITO OU QUALQUER OUTRA TEORIA DO DIREITO, POR QUALQUER PREJUÍZO ESPECIAL, ACIDENTAL OU CONSEQÜENCIAL, SEJA QUAL FOR, INCLUINDO, SEM LIMITAÇÃO, PREJUÍZOS POR PERDA DE LUCROS, INTERRUPÇÃO DE NEGÓCIOS, DANOS PESSOAIS, PERDA OU DETERIORAÇÃO DE DADOS OU DE INFORMAÇÕES COMERCIAIS, AINDA QUE A SSN TENHA SIDO NOTIFICADA DA POSSIBILIDADE DE OCORRÊNCIA DE TAIS PREJUÍZOS. A RESPONSABILIDADE DA SSN (SE HOUVER) POR PREJUÍZOS DIRETOS DE QUALQUER CAUSA, SEJA QUAL FOR, E SEM LEVAR EM CONSIDERAÇÃO A FORMA DA AÇÃO, ESTARÁ LIMITADA A E NÃO EXCEDERÁ O MONTANTE PAGO PELO HARDWARE/SOFTWARE.

3. **Informações gerais** Esta licença de software a garantia limitada será coberta e interpretada de acordo com as leis do Estado do Texas, EUA (excluindo conflitos de regras de leis), e terá efeito para o benefício da SSN e seu sucessor, seus procuradores e representantes legais. Se qualquer cláusula desta licença de software e garantia limitada for interpretada por um tribunal legalmente qualificado como inválida ou que não possa ser aplicada dentro de qualquer limite da lei aplicável, essa cláusula será aplicada no limite máximo admissível e as cláusulas restantes desta licença de software e garantia limitada permanecerão em pleno vigor e efeito. Quaisquer notificações ou outras comunicações a serem enviadas para a SSN devem ser postadas por carta registrada ao seguinte endereço:

Siemens Subscriber Networks

4849 Alpha Road

Dallas, TX 75244

U.S.A.

Attn: Customer Service

# Índice


**CAPÍTULO 1** ..... **4**

**INTRODUÇÃO** ..... **4**

**Recursos do roteador SpeedStream®** ..... **4**
Recursos da rede local ..... 4
Recursos de segurança ..... 4
Configuração e gerenciamento ..... 5
Funções avançadas do roteador ..... 5
**Requisitos mínimos do sistema** ..... **5**
**Recomendações gerais de segurança** ..... **6**

**CAPÍTULO 2** ..... **7**

**INSTALAÇÃO FÍSICA** ..... **7**

**Requisitos mínimos do sistema** ..... **7**
**Instalação do hardware** ..... **7**
Procedimento básico de instalação ..... 7
Instalação dos filtros de linha ..... 8
Conexão de cabos ..... 9

**CAPÍTULO 3** ..... **12**

**CONFIGURAÇÃO DO SISTEMA OPERACIONAL** ..... **12**

**Verificação das configurações do protocolo TCP/IP** ..... **12**
Verificação das configurações do TCP/IP (Windows 9x/ME) ..... 13
Verificação das configurações do TCP/IP (Windows 2000) ..... 14
Verificação das configurações do TCP/IP (Windows XP) ..... 15
Verificação das configurações do TCP/IP (MAC OS 8.6 a 9.x) ..... 16
Verificação das configurações do TCP/IP (MAC OSX) ..... 17
**Configuração do acesso à Internet** ..... **18**
Para Windows 9x/2000 ..... 18
Para Windows XP ..... 18

**CAPÍTULO 4** ..... **19**

**CONFIGURAÇÃO DO ROTEADOR SPEEDSTREAM** ..... **19**

**Antes de configurar o roteador** ..... **19**
**Conexão ao roteador** ..... **20**
Seleção da conexão PPP ..... 21
Login PPP ..... 22
**Janela inicial** ..... **23**

**CAPÍTULO 5** ..... **24**

**CONFIGURAÇÃO DOS PERFIS DE USUÁRIO** ..... **24**

**Inclusão de perfis de usuário** ..... **24**
**Edição de perfis de usuário** ..... **28**
**Exclusão de perfis de usuário** ..... **28**

**CAPÍTULO 6** ..... **29**

**CONFIGURAÇÃO DA CONEXÃO DO PROVEDOR DE SERVIÇO INTERNET** ..... **29**

**Interface WAN** ..... **29**
**Host** ..... **30**
**DHCP** ..... **31**
**Rotas estáticas** ..... **33**
**RFC2684** ..... **34**

**CAPÍTULO 7** ..... **35**

**DEFINIÇÃO DA CONFIGURAÇÃO DE REDE** ..... **35**

Protocolo RIP ..... 36
Redirecionamento de porta ..... 37
UPnP (Universal Plug and Play) ..... 38
Modo Bridge ..... 39
Portas do servidor ..... 40
DNS dinâmico ..... 41

**CAPÍTULO 8** ..... **42**

**CONFIGURAÇÃO DOS RECURSOS DE SEGURANÇA** ..... **42**

Usuário admin ..... 43
**Time Client** ..... **44**
**Servidor NAT/NAPT** ..... **45**
**Firewall** ..... **46**
Nível ..... 47
Intervalo de espera (snooze) ..... 49
DMZ ..... 50
Regras de filtragem ..... 51
**Registro (Log)** ..... **57**
**ADS** ..... **58**

**CAPÍTULO 9** ..... **60**

**MONITORAMENTO DO ESTADO DO ROTEADOR** ..... **60**

**Status e estatísticas** ..... **60**
Resumo do sistema ..... 61
Log do sistema ..... 61
**Diagnóstico** ..... **65**
**Ferramentas** ..... **66**
Mapa de interface ..... 66
Reinicialização ..... 67
Atualização ..... 68

**APÊNDICE A** ..... **69**

**SOLUÇÃO DE PROBLEMAS** ..... **69**

**Etapas para a solução de problemas básicos** ..... **69**
**Interpretação do mostrador de LED** ..... **70**
**Solução de problemas específicos** ..... **71**
Falha de POST (LED *pwr* vermelho) ..... 71
**Contato com o suporte técnico** ..... **72**

**APÊNDICE B ..... 73**

**NÍVEIS DE SEGURANÇA DO FIREWALL ..... 73**

# Capítulo 1

# Introdução

Parabéns pela aquisição do roteador SpeedStream® com SecureRoute™. O roteador SpeedStream® é um dispositivo de comunicação poderoso, porém simples de usar, para conectar o seu computador ou rede local (LAN) à Internet. Este manual abrange os roteadores SpeedStream modelos 4100 e 4200.

**SpeedStream 4100 (Ethernet)**

**SpeedStream 4200 (Ethernet e USB)**

## Recursos do roteador SpeedStream®

O roteador fornece acesso de alta velocidade à Internet e à rede corporativa para residências, home offices interligados em rede e pequenos escritórios. Além disso, se você estiver trabalhando em uma filial, o roteador fornece um meio rápido e eficaz de comunicação com a matriz através de uma rede LAN remota. O roteador pode ser usado também para conectar a rede LAN corporativa à Internet através da rede remota (WAN).

### Recursos da rede local

- **Switch Ethernet**
  Conectividade Ethernet (em todos os modelos) à Internet ou à rede através de uma placa de rede (NIC), fornecendo largura de banda total de 10/100 megabits por segundo (Mbps) até a porta.
- **Conexão USB**
  Conexão (no modelo 4200) através de barramento serial universal (USB) fornecendo flexibilidade adicional para a conexão do computador via porta Ethernet ou USB.
- **Suporte a G.lite e Full-Rate DSL**
  Assegura a compatibilidade com a maioria das redes DSL.

### Recursos de segurança

- **Configuração protegida por senha**
  A proteção por senha evita que usuários não autorizados modifiquem os ajustes de configuração do roteador.
- **Segurança por firewall**
  Segurança por firewall com quatro níveis de segurança padrão convenientemente pré-configurados (desligado, baixo, média, alto), um modo compatível com ICSA e um ajuste de configuração personalizado para usuários avançados.
- **Proteção por NAT**
  Conversão de porta de endereço de rede (NAPT) e um firewall seguro para proteger os seus dados enquanto o computador estiver conectado à Internet.
- **Firewall com tecnologia Stateful Inspection**
  Todos os pacotes de dados de entrada e todas as solicitações recebidas pelo servidor são filtrados, protegendo assim a rede contra ataques maliciosos de fontes externas.

- **Sistema de proteção contra ataques**
  Os ataques podem sobrecarregar a conexão à Internet com solicitações de conexão e pacotes de dados inválidos, usando todos os recursos de largura de banda e tornando o acesso à Internet indisponível. O roteador incorpora a proteção contra esses tipos de ataques assim como a outros ataques comuns de hackers.
- **Rede virtual privada (VPN)**
  A rede virtual privada permite a usuários remotos estabelecer uma conexão segura com uma rede corporativa pela configuração da conexão por meio de um dos três protocolos VPN mais utilizados: PPTP, L2TP e IPSec.

### Configuração e gerenciamento

- **Fácil configuração**
  Use o seu navegador da Web para uma configuração fácil e rápida.
- **Suporte a UpnP**
  O Universal Plug and Play (UPnP) permite a descoberta automática e a configuração do roteador SpeedStream. O UPnP é suportado nos sistemas operacionais Windows ME, XP ou posteriores.

### Funções avançadas do roteador

- **DMZ**
  Um computador conectado à rede local pode ser configurado para permitir comunicação bidirecional irrestrita com servidores ou usuários individuais na Internet. Isso oferece a capacidade de executar programas incompatíveis com firewalls.
- **Redirecionamento de porta**
  O redirecionamento de porta fornece flexibilidade ao permitir que você altere o endereço IP interno sem afetar o acesso externo à sua rede.
- **Controle de sessão**
  Alguns protocolos, como FTP, exigem conexões secundárias de rede a outras portas além da porta de controle principal. Essas conexões são normalmente estabelecidas com o uso de números de porta no intervalo dinâmico (> 1024). O firewall permite o tráfego em sessões secundárias sem a necessidade de configuração manual.

## Requisitos mínimos do sistema

O computador deve estar equipado com os requisitos mínimos descritos a seguir para uma instalação bem sucedida do roteador. O seu provedor de serviços de Internet pode ter requisitos adicionais para o uso do serviço.

- **Método de conexão via Ethernet**
  - Uma placa de rede (NIC) com suporte a Ethernet 10/100Base-T full/half-duplex.
  - Sistema operacional com suporte a TCP/IP.
  - Microsoft Internet Explorer ou Netscape Navigator nas versões 5.0 ou posterior..
- **Método de conexão via USB**
  - 32 MB de RAM
  - Processador Pentium compatível de 166 MHz (ou mais rápido).
  - 12 MB de espaço disponível em disco.
  - Sistema operacional Windows 98 ou posterior.

## Recomendações gerais de segurança

Ao utilizar o roteador SpeedStream, observe as recomendações de segurança a seguir:

- Nunca instale cabos de telefone durante uma tempestade.
- Evite usar um aparelho telefônico durante uma tempestade elétrica. A incidência de raios aumenta o risco de choque elétrico.
- Não instale tomadas de telefone em locais molhados e nunca use o aparelho próximo à água.
- Não ultrapasse os valores nominais máximos de tensão de alimentação do produto.

# Capítulo 2

# Instalação física

*Este capítulo abrange a instalação física do roteador SpeedStream.*

## Requisitos mínimos do sistema

- Serviço DSL e uma conta de acesso à Internet de um provedor de serviços Internet (ISP).
- Cabos de rede do dispositivo a ser conectado ao roteador. Use cabos Ethernet padrão CAT5 com conectores RJ45.
- O protocolo de rede TCP/IP deve estar instalado em todos os computadores.
- Para uma conexão ao roteador via USB, os seguintes sistemas operacionais são suportados (se o seu modelo de roteador suporta USB):
  - Windows 98, 98SE
  - Windows 2000
  - Windows ME ou XP
  - Mac OS nas versões 8.6 até 10.2.4

**Nota:** As instruções e ilustrações de configuração neste capítulo podem variar ligeiramente. Consulte a documentação ou contate o seu provedor de serviços sobre dúvidas relativas à configuração específica.

## Instalação do hardware

O roteador SpeedStream pode ser instalado em qualquer local conveniente de seu escritório ou residência. Não há necessidade de fiação ou ventilação especial, contudo, é necessário obedecer as normas de segurança especificadas na seção Recomendações gerais de segurança.

### Procedimento básico de instalação

1. Instalar os filtros de linha, se necessário.
2. Conectar os cabos.
3. Instalar os drivers USB, se necessário.
4. Definir as configurações de rede em seu computador.
5. Configurar o roteador através da interface de gerenciamento baseada na Web.
6. Reinicialize o computador quando solicitado. Sempre que for necessário reinicializar o roteador, aguarde cinco segundos após desligar a unidade antes de ligá-la novamente.

## Instalação dos filtros de linha

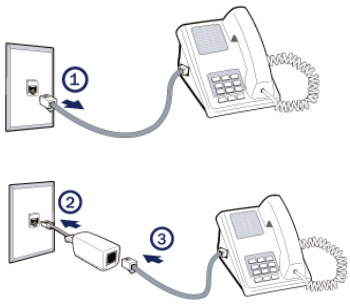
Uma vez que o tráfego DSL compartilha a sua linha telefônica, pode ser necessário separar os dois sinais de forma que não interfiram entre si. Um microfiltro (incluso em alguns modelos) evita interferências do tráfego DSL em sua linha telefônica e vice-versa. Siga os procedimentos abaixo para instalar filtros de linha em qualquer dispositivo (telefones, máquinas de fax, identificadores de chamada) que compartilhe a mesma linha telefônica com o seu DSL.

(Note que esta seção pode não ser aplicável no seu caso. Consulte o seu provedor de serviços se não tiver certeza).

Há dois tipos de filtros para a conexão entre o telefone e a tomada telefônica de parede:

- *Microfiltro:* Para uso com aparelhos telefônicos convencionais de mesa.
- *Filtro de montagem em parede:* Para uso com aparelhos telefônicos de montagem em parede.

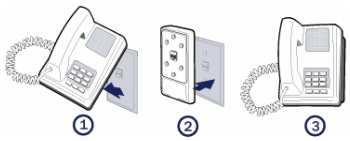
O desempenho do DSL pode ser degradado de forma significativa se os filtros de linha não estiverem instalados no sentido correto como ilustrado abaixo.




**Microfiltro**

Para cada dispositivo que compartilhar a mesma linha telefônica:

1. Desconecte o cabo do dispositivo da tomada do telefone.
2. Conecte o microfiltro à tomada do telefone.
3. Conecte o cabo do telefone (ou de outro dispositivo) ao microfiltro.




**Filtro de montagem em parede**

Para um telefone de montagem em parede, instale um filtro de montagem em parede:

1. Remova o telefone.
2. Conecte o filtro de montagem em parede no suporte de parede.
3. Reconecte o telefone.

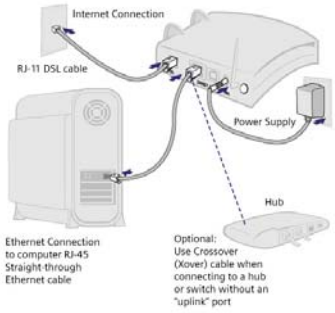
## Conexão de cabos

O roteador fornece portas para uma conexão USB ou Ethernet ao seu computador principal. Selecione a interface que será utilizada para conectar o roteador e siga as instruções passo a passo descritas abaixo para o método de instalação escolhido.

## Método de instalação por Ethernet

Para conectar o roteador SpeedStream através da interface Ethernet, é necessário que o seu computador tenha um adaptador Ethernet (também chamado de placa de rede ou “NIC”) instalado.

Caso o seu computador não tenha este adaptador, instale-o antes de prosseguir. Consulte a documentação do seu adaptador Ethernet para obter instruções de instalação detalhadas.


Internet Connection
RJ-11 DSL cable
Power Supply
Hub
Ethernet Connection to computer RJ-45 Straight-through Ethernet cable
Optional: Use Crossover (Xover) cable when connecting to a hub or switch without an "uplink" port

**1. Conecte o(s) cabo(s) Ethernet:**

1) Com o computador desligado, conecte o cabo Ethernet a uma porta Ethernet (1-4) do roteador.

2) Conecte a outra extremidade do cabo Ethernet à porta Ethernet de seu computador.

3) Se necessário, use cabos Ethernet padrão CAT5 10/100 para conectar mais computadores às portas restantes no roteador.

**2. Conecte o cabo DSL:**

1) Conecte o cabo DSL (parecido com fio telefônico) à porta DSL do roteador.

Conecte a outra extremidade do cabo DSL à tomada do telefone.

**3. Conecte a alimentação:**

1) Conecte a fonte de alimentação na parte traseira do roteador.

2) Ligue a fonte de alimentação à tomada de energia elétrica.

3) Pressione a chave liga/desliga para ligar o roteador SpeedStream. Ligue todos os computadores conectados.

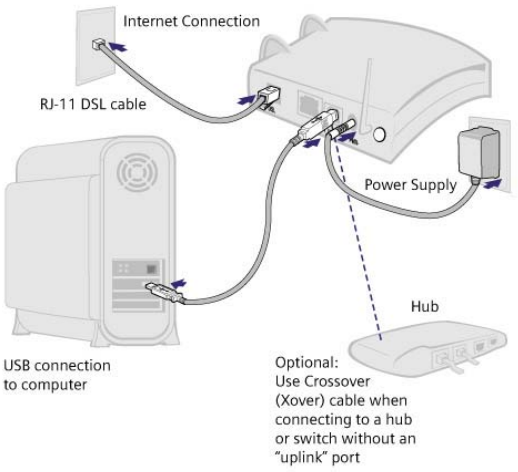
**4. Verifique os LEDs:**

1) Para cada conexão Ethernet ativa, o LED de link de rede (LAN link) do número da porta correspondente deve estar aceso.

2) Os LEDs de DSL e de alimentação (Power) devem estar acesos.

Ao usar o método de instalação de Ethernet, não é necessário instalar nenhum software. Consulte as instruções do seu provedor de serviços Internet para a instalação do software e/ou conexão à Internet. É possível definir as configurações de TCP/IP como detalhadas no Capítulo 3, Configuração do sistema operacional.

## Método de instalação de USB (Microsoft Windows)


Internet Connection
RJ-11 DSL cable
Power Supply
Hub
USB connection to computer
Optional: Use Crossover (Xover) cable when connecting to a hub or switch without an "uplink" port

**1. Conecte o cabo USB:**

1) Com o computador desligado, conecte o cabo USB fornecido à porta USB do roteador.
2) Conecte a outra extremidade do cabo USB a uma porta USB livre de seu computador.
3) Se desejar, use cabos Ethernet padrão CAT5 10/100 para conectar outros computadores às portas Ethernet do roteador.

**2. Conecte o cabo DSL:**

1) Conecte o cabo DSL (parecido com fio telefônico) à porta DSL do roteador.
2) Conecte a outra extremidade do cabo DSL à tomada do telefone.

**3. Conecte a alimentação:**

1) Conecte a fonte de alimentação na parte traseira do roteador.
2) Ligue a fonte de alimentação à tomada de energia elétrica.
3) Pressione a chave liga/desliga para ligar o roteador.
4) Ligue todos os computadores conectados.

**4. Instale o software do driver USB:**

1) Insira o CD-ROM do driver USB na unidade de CD-ROM do seu computador.
2) Quando solicitado, siga as instruções exibidas na tela para concluir a instalação do driver.

**5. Verifique os LEDs:**

1) Os LEDs de DSL e de alimentação (Power) devem estar acesos.

É possível definir as configurações de TCP/IP como detalhadas no Capítulo 3, Configuração do sistema operacional.

## Instalação do driver USB (Macintosh)

Ao usar o método de instalação de USB em um Macintosh, siga os passos abaixo para instalar os drivers USB:

**1.** Insira o CD de instalação do SpeedStream® na unidade de CD-ROM.

2. Abra o ícone SpeedStream® na área de trabalho.

3. Clique em Readme.txt para abri-lo.
4. Siga as instruções exibidas no arquivo Readme.txt.

É possível definir as configurações de TCP/IP como detalhadas no Capítulo 3, Configuração do sistema operacional.

# Capítulo 3

# Configuração do sistema operacional

*Este capítulo explica como configurar o seu computador para funcionar com o roteador.*

Para ter acesso à Internet por meio do roteador SpeedStream, é necessário que o protocolo TCP/IP esteja instalado em seu computador. Se o protocolo TCP/IP não estiver instalado em seu computador, consulte a documentação do seu sistema ou a ajuda on-line para obter instruções. Uma vez instalado, você deve verificar as configurações do protocolo TCP/IP para ter certeza que estejam corretas para o uso com o roteador.

Com o TCP/IP instalado e configurado corretamente, a próxima etapa é preparar o seu computador para usar o roteador no acesso à Internet configurando o navegador da Web para ter acesso à Internet através da rede local (LAN), e não pela conexão dial-up.

## Verificação das configurações do protocolo TCP/IP

Uma vez que o roteador usa o protocolo TCP/IP para todas as funções, é essencial que o protocolo TCP/IP esteja instalado e configurado corretamente.

As configurações de rede padrão do roteador SpeedStream são as seguintes:

| | |
|---|---|
| Endereço IP: | 192.168.254.254 |
| Máscara de sub-rede: | 255.255.255.0 |

Se as configurações padrão do roteador e do TCP/IP do Windows forem utilizadas, não será necessário efetuar nenhuma alteração.

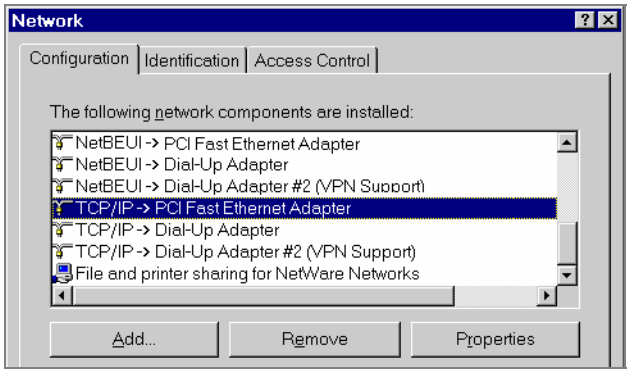
Como padrão, o roteador agirá como um servidor DHCP, fornecendo automaticamente um endereço IP apropriado e as informações relacionadas para cada computador inicializado. Por padrão, para todas as versões do Windows que não sejam do tipo servidor, a configuração do TCP/IP age como um cliente DHCP.

As instruções de verificação das configurações do protocolo TCP/IP são diferentes para cada sistema operacional. Verifique as configurações usando as instruções para o seu sistema operacional:

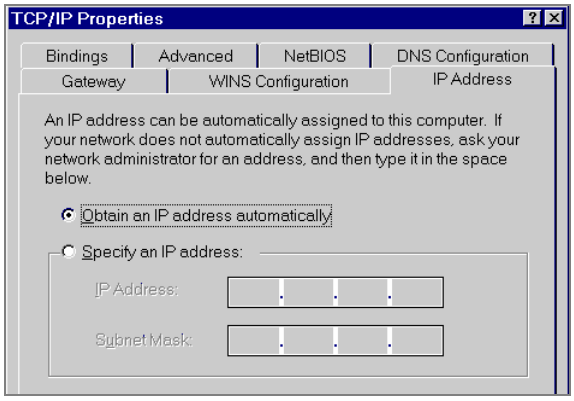
- Windows 9x/ME
- Windows 2000
- Windows XP
- MAC OS 8.6 até 9.x
- MAC OSX

## Verificação das configurações do TCP/IP (Windows 9x/ME)

1. Clique em **Iniciar > Painel de controle > Rede**. A guia **Configuração** na janela “Rede” é exibida.



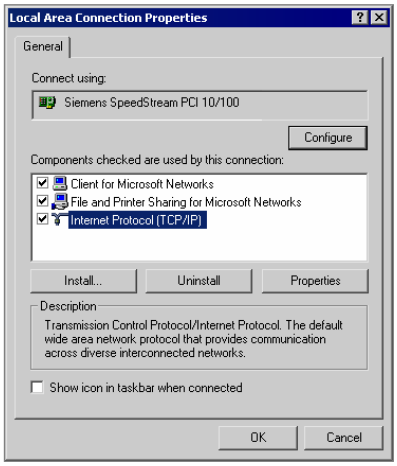

2. Selecione o protocolo TCP/IP para a sua placa de rede.
3. Clique em **Propriedades**. A janela “Propriedades de TCP/IP” é exibida.

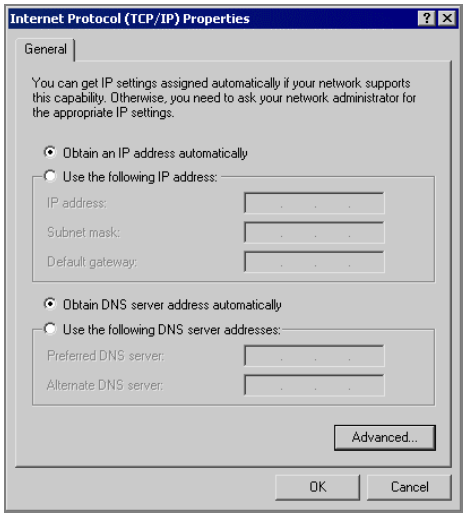

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:

4. Clique na guia **Endereço IP**.
5. Certifique-se de que a opção **Obter um endereço IP automaticamente** está selecionada. Essa é a configuração padrão do Windows.
6. Feche a janela.
7. Reinicialize o computador para obter um endereço IP do roteador.
8. Configure o acesso à Internet utilizando o procedimento descrito em Configuração do acesso à Internet.

## Verificação das configurações do TCP/IP (Windows 2000)

1. Na barra de tarefas, clique em **Iniciar > Configurações > Painel de controle**. A janela “Painel de controle” é exibida.
2. Clique duas vezes em **Conexões dial-up e de rede**. A janela “Conexões dial-up e de rede” é exibida.
3. Clique com o botão direito em **Conexão de rede local** e selecione **Propriedades**. A janela “Propriedades de conexão de rede local” é exibida.
4. Selecione o protocolo TCP/IP para a sua placa de rede.
5. Clique em **Propriedades**. A janela “Propriedades de protocolo Internet (TCP/IP)” é exibida.

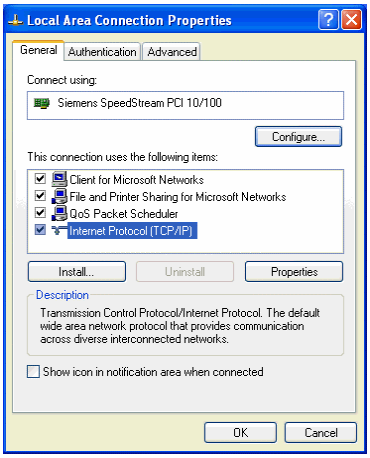


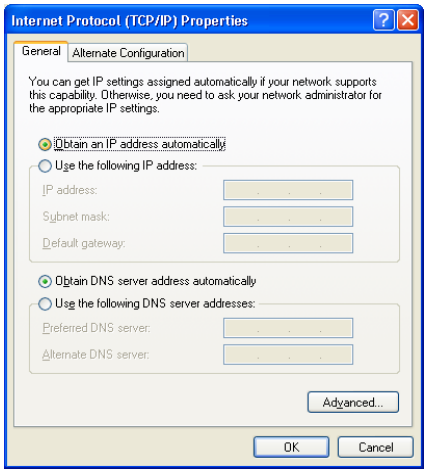


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6. Selecione as opções Obter um endereço IP automaticamente e Obter o endereço dos servidores DNS. Feche o painel de controle.
7. Reinicialize o computador para obter um endereço IP do roteador.
8. Configure o acesso à Internet utilizando o procedimento descrito em Configuração do acesso à Internet.

## Verificação das configurações do TCP/IP (Windows XP)

1. Na barra de tarefas, clique em **Iniciar > Painel de controle**. A janela “Painel de controle” é exibida.
2. Clique duas vezes no ícone **Conexões de rede**. A janela “Conexões de rede” é exibida.
3. Clique com o botão direito em **Conexão de rede local** e, em seguida, clique em **Propriedades**. A janela “Propriedades de conexão de rede local” é exibida.
4. Selecione o protocolo TCP/IP para a sua placa de rede.
5. Clique em **Propriedades**. A janela “Propriedades de protocolo Internet (TCP/IP)” é exibida.

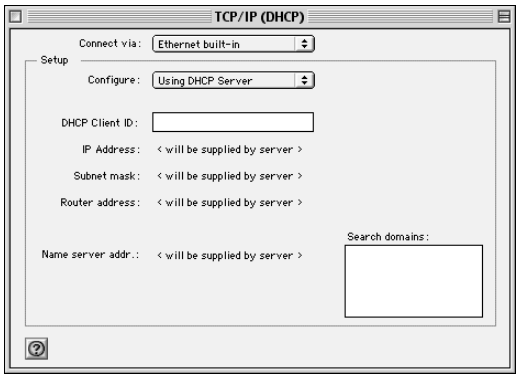




Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6. Certifique-se de que as opções Obter um endereço IP automaticamente e Obter o endereço dos servidores DNS estão selecionadas.
7. Feche o painel de controle.
8. Reinicialize o computador para obter um endereço IP do roteador.
9. Configure o acesso à Internet utilizando o procedimento descrito em Configuração do acesso à Internet.

## Verificação das configurações do TCP/IP (MAC OS 8.6 a 9.x)

1. Clique em **Apple > Painel de controle > TCP/IP**. A janela “TCP/IP” é exibida.




2. Selecione uma das opções seguintes no menu **Conectar via**.
   - **Ethernet** ou **Ethernet incorporada** se a conexão for via Ethernet.
   - **Adaptador Ethernet [en0, en1,...]** se a conexão for via USB.
3. Selecione Utilizando o servidor DHCP no menu suspenso Configurar.
4. Feche a janela “TCP/IP” e clique em **Salvar**.
5. Reinicialize após salvar a configuração. Após a reinicialização, o computador solicitará um endereço IP do servidor DHCP no roteador.
6. Configure o roteador utilizando o procedimento descrito no próximo capítulo.

## Verificação das configurações do TCP/IP (MAC OSX)

1. Clique em **Apple > Preferências do sistema**. A janela “Preferências do sistema” é exibida.

2. Clique duas vezes no ícone **Rede** na seção **Internet e Rede**. A janela “Rede” é exibida.

3. Selecione uma das opções seguintes no menu **Mostrar**:
   - **Ethernet incorporada**, se a conexão for via Ethernet.
   - **Adaptador Ethernet [en0, en1,...]** se a conexão for via USB.
4. Selecione Utilizando o servidor DHCP no menu Configurar IPv4.
5. Clique em **Aplicar agora** e feche a janela.
6. Configure o roteador utilizando o procedimento descrito no próximo capítulo.

# Configuração do acesso à Internet

Os usuários do Windows devem configurar o computador para utilizar o roteador no acesso à Internet. Certifique-se que o roteador esteja instalado corretamente e se a linha DSL está funcional. Em seguida, siga o procedimento adequado abaixo para configurar o seu navegador da Web para ter acesso à Internet através da rede local (LAN) e não através da conexão dial-up.

## Para Windows 9x/2000

1. Clique em **Iniciar > Configurações > Painel de Controle** para exibir o painel de controle.
2. Clique duas vezes no ícone **Opções da Internet**. A janela “Propriedades de Internet” é exibida.
3. Selecione a guia **Conexões**.
4. Clique em **Configurar**.
5. Selecione **Desejo configurar uma conexão com a Internet manualmente ou através de uma rede local** e, em seguida, clique em **Avançar**. A janela “Assistente para a conexão com a Internet” é exibida.
6. Selecione **Através de uma rede local (LAN)** e, em seguida, clique em **Avançar**. A janela “Configuração de rede local na Internet” é exibida.
7. Certifique-se de que todas as caixas de seleção estejam desmarcadas e, em seguida, clique em **Avançar**. A janela “Configure sua conta no Internet Mail” é exibida.
8. Selecione **Não** e, em seguida, clique em **Avançar**. A janela “Concluindo o assistente para a conexão com a Internet” é exibida.
9. Clique em **Concluir** para fechar o Assistente para conexão com a Internet. A configuração está concluída.
10. Configure o roteador utilizando o procedimento descrito no próximo capítulo.

## Para Windows XP

1. Clique em Iniciar > Painel de controle.
2. Clique duas vezes no ícone **Opções da Internet**. A janela “Propriedades de Internet” é exibida.
3. Selecione a guia **Conexões**.
4. Clique em Configurar. O Assistente para novas conexões será iniciado.
5. Clique em **Avançar**.
6. Selecione **Conectar-me à Internet** e, em seguida, clique em **Avançar**.
7. Selecione Configurar minha conexão manualmente e, em seguida, clique em Avançar.
8. Selecione Conectar-me usando uma conexão de banda larga sempre ativa e, em seguida, clique em Avançar.
9. Clique em **Concluir**.
10. Configure o roteador utilizando o procedimento descrito no próximo capítulo.

# Capítulo 4

# Configuração do roteador SpeedStream

*Este capítulo fornece detalhes dos processos de configuração do roteador.*

Este capítulo descreve as etapas para definir a configuração do roteador SpeedStream com o uso do Assistente de configuração do roteador. Pode ser necessária também outra configuração no roteador, dependendo de quais recursos e funções do roteador SpeedStream você deseja utilizar. Use a tabela abaixo para localizar instruções detalhadas para as funções desejadas.

| **Para:** | **Consulte:** |
|---|---|
| Configurar usuários no roteador. | Capítulo 5, “Configuração dos perfis de usuário” |
| Definir parâmetros de configuração do provedor de serviços de Internet. Isso deve ser feito apenas sob orientação do seu provedor de serviços de Internet. | Capítulo 6, “Definição da configuração de conexão do ISP” |
| Configurar as informações relativas à rede. | Capítulo 7, “Definição da configuração de rede” |
| Adicionar segurança à rede. | Capítulo 8, “Configuração dos recursos de segurança” |
| Monitorar o estado do roteador. | Capítulo 9, “Monitoramento do estado do roteador” |

## Antes de configurar o roteador

Antes de configurar o roteador, certifique-se de que:

- O seu computador estabelece uma conexão física com o roteador. O computador e o roteador estão conectados diretamente pela porta USB ou porta Ethernet no roteador.
- O roteador SpeedStream está instalado corretamente e ligado.
- O protocolo TCP/IP está instalado em todos os computadores de sua rede. (Se for necessário instalar o TCP/IP, consulte a documentação do sistema na ajuda do Windows).
- Se as configurações de rede em cada computador estão corretas.

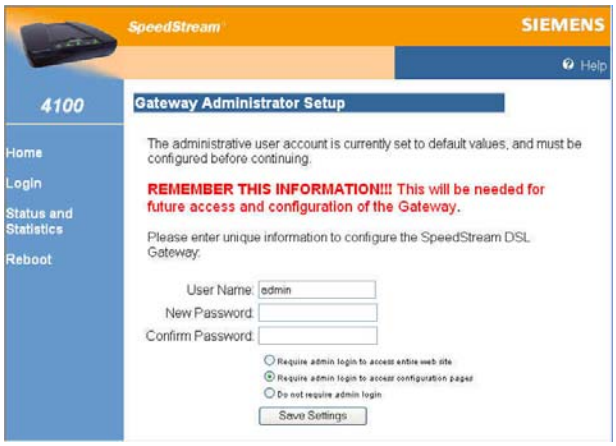
Desse ponto em diante, toda a configuração do roteador SpeedStream em seu computador será feita por meio de um programa de configuração baseado em um navegador da Web.

## Conexão ao roteador

O roteador SpeedStream contém um servidor HTTP que permite conectá-lo e efetuar sua configuração a partir de seu navegador da Web (Microsoft Internet Explorer ou Netscape Navigator, versões 5.0 ou posteriores).

Para estabelecer uma conexão de seu computador ao roteador:

1. Após instalar o roteador, inicie o seu computador. Se o computador já estiver ligado, reinicialize-o.
2. Abra o seu navegador na Web (Internet Explorer ou Netscape Navigator).
3. Na barra **Endereço**, digite o endereço IP padrão do roteador: **http://speedstream** e pressione **Enter**. A janela “Gateway Administrator Setup” (Configuração do administrador de gateway) é exibida.


SpeedStream
SIEMENS
Help
4100
Gateway Administrator Setup
Home
Login
Status and Statistics
Reboot
The administrative user account is currently set to default values, and must be configured before continuing.
REMEMBER THIS INFORMATION!!! This will be needed for future access and configuration of the Gateway.
Please enter unique information to configure the SpeedStream DSL Gateway.
User Name: admin
New Password:
Confirm Password:
Require admin login to access entire web site
Require admin login to access configuration pages
Do not require admin login
Save Settings

Ao conectar-se ao roteador pela primeira vez com o navegador da Web, será necessário configurar uma conta de administrador na janela “Configuração do administrador de gateway” antes de prosseguir.

4. Especifique um nome de usuário para o administrador. Você pode aceitar o nome de usuário padrão **admin** ou digitar um novo nome de usuário em **User name** (Nome de usuário). O nome de usuário distingue entre maiúsculas e minúsculas.
5. Digite uma senha em **New Password** (Nova senha) e a mesma senha em **Confirm New Password** (Confirmar nova senha). O campo de senha distingue entre maiúsculas e minúsculas.
6. Selecione um nível de segurança de login dentre os relacionados a seguir:
   - **Require admin login to access entire Web site** (Requer login de administrador para ter acesso a todo o site da Web)
     Antes de ter acesso a qualquer tela na interface da Web, é necessário efetuar o login com o seu nome de usuário e senha na rede. (nível de segurança = alto)
   - **Require admin login to access configuration pages** (Requer login de administrador para ter acesso às paginas de configuração)
     Antes de acessar qualquer tela na interface da Web que permita alterar a configuração, é necessário efetuar o login com o seu nome de usuário e senha na rede. (nível de segurança = médio)
   - **Não requer login de administrador:**
     Após efetuar o login pela primeira vez, não será mais necessário efetuar o login novamente em qualquer tela. (nível de segurança = baixo)
7. Clique em **Save Settings** (Salvar configurações). Dependendo da(s) conexão(ões), será exibida uma das seguintes telas:

- Se não houver conexões ponto a ponto (PPP) configuradas, a tela **System Summary** (Resumo do sistema) será exibida.
- Se uma conexão ponto a ponto (PPP) for configurada, a tela **Login PPP** será exibida para a conexão. Consulte Login PPP para obter mais detalhes.
- Se houver diversas conexões ponto a ponto (PPP) configuradas, a tela **PPP Login [choose connection]** (Login PPP [escolher a conexão]) exibirá as conexões disponíveis. Consulte Selecionar conexão PPP para obter mais detalhes.

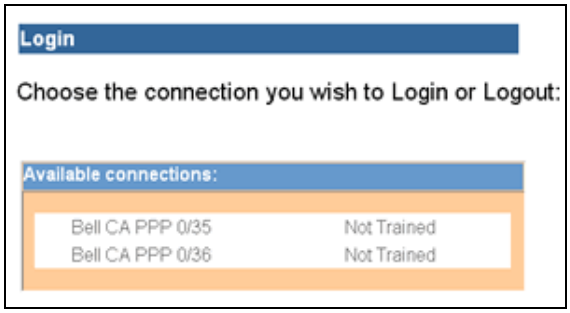
O ponto a ponto oferece o recurso de Conexão sob demanda pelo qual o roteador tentará conectar-se a uma sessão PPP desconectada se houver solicitação de tráfego pela rede LAN, e se houver um nome de usuário e senha salvos. Isso é particularmente útil com o recurso Idle Timeout (Tempo limite de inatividade). A conexão sob demanda não é configurável, mas está sempre ativada.

8. Caso você tenha selecionado outra opção que exige login de administrador, será necessário efetuar novamente o login para obter a permissão de executar qualquer atividade. Ao selecionar qualquer opção de menu, a janela de login a seguir será exibida.

9. Digite o nome de usuário e a senha atribuída ao administrador para executar as atividades de configuração restantes.
10. Clique em **OK**. A tela da opção de menu selecionada é exibida.
11. Consulte os capítulos seguintes para obter detalhes da configuração e do gerenciamento do roteador SpeedStream.

## Seleção da conexão PPP

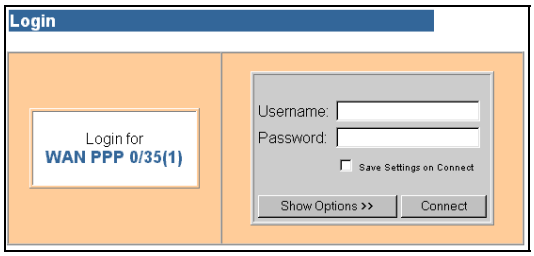
Se houver várias sessões PPP (ponto a ponto) configuradas em seu computador, a janela “Login” será exibida com as conexões PPP disponíveis após o login na janela “Configuração do usuário administrativo”.


Login
Choose the connection you wish to Login or Logout:
Available connections:
Bell CA PPP 0/35 Not Trained
Bell CA PPP 0/36 Not Trained

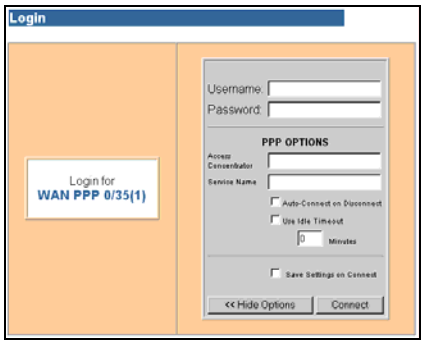
Clique na conexão desejada.

## Login PPP

Se apenas uma sessão PPP (ponto a ponto) for tiver sido configurada no computador, a janela “Login” será exibida para essa conexão PPP após o login na janela “Administrative User Setup” (Configuração do usuário administrativo).



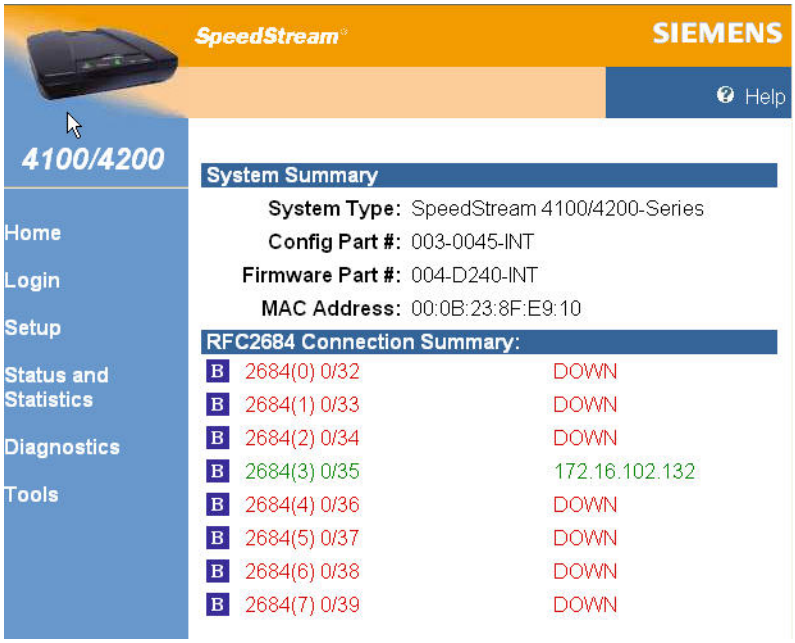

1. Na janela **Login PPP**, digite o nome de usuário e a senha.
2. Para salvar as configurações de modo que não seja necessário informar o nome de usuário e a senha no futuro, clique em **Save Settings on Connect** (Salvar configurações ao conectar).
3. Para configurar opções PPP adicionais, clique em **Show Options** (Mostrar opções). A janela será expandida para exibir as opções configuráveis da conexão PPP.




4. Marque uma das opções PPP desejadas a seguir:
   - **Access Concentrator** (Concentrador de acesso)
     Digite o nome do concentrador de acesso fornecido pelo provedor de serviços Internet.
   - **Service Name** (Nome do serviço)
     Digite o nome do serviço fornecido pelo provedor de serviços de Internet.
   - **Auto-Connect on Disconnect** (Conectar automaticamente ao desconectar)
     Caso a opção esteja marcada, o roteador tentará efetuar o login sempre que o DSL for exibido após selecionar **Save Settings on Connect** (Salvar configurações ao conectar).
   - **Idle Timeout (with time value)** (Tempo limite de inatividade (com valor de tempo)
     Marque esta opção para desconectar a sessão PPP caso não haja tráfego no roteador por um determinado período de tempo. Digite o tempo em minutos (esta opção não pode ser usada com a conexão automática).

## Janela inicial

Após a primeira inicialização, a janela inicial (Home) é exibida.




O painel de navegação à esquerda da janela inicial possui opções de configuração, diagnóstico, status e estatística do roteador. A lista de opções exibidas pode ser diferente dependendo do login usado pelo usuário no sistema. Um administrador possui plenos direitos de configurar e visualizar um conjunto de opções (mostrados acima), ao passo que um usuário possui direitos de configuração limitados e visualizará o subconjunto definido para o seu perfil.

Consulte os capítulos seguintes para obter informações sobre como usar cada uma destas opções.

- Consulte o Capítulo 5, “Configuração dos perfis de usuário”, para obter detalhes sobre inclusão, modificação ou exclusão de perfis de usuário.
- Consulte o Capítulo 6: “Definição da configuração de conexão do ISP”, para obter detalhes sobre definição de parâmetros de configuração do provedor de serviços Internet. Isso deve ser feito apenas sob orientação do seu provedor de serviços de Internet.
- Consulte o Capítulo 7, “Definição da configuração de rede”, para obter detalhes das informações relacionadas à configuração da rede.
- Consulte o Capítulo 8, “Configuração dos recursos de segurança” para obter detalhes sobre a melhoria da segurança na sua rede.
- Consulte o Capítulo 9, “Monitoramento do estado do roteador”, para obter detalhes sobre a visualização de estatísticas da rede e do status de conexão.

# Capítulo 5

# Configuração dos perfis de usuário

*Este capítulo contém detalhes da configuração de usuários no roteador SpeedStream.*

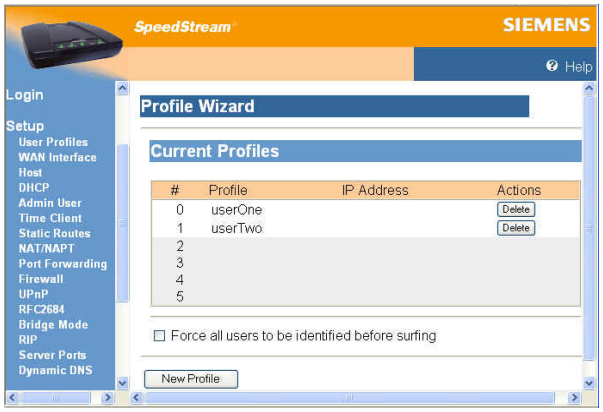
Os perfis de usuário são utilizados para controlar o roteador e o acesso à rede por usuários individuais. O acesso à configuração e gerenciamento do roteador deve ser restrito apenas a usuários autorizados. Este capítulo descreve como:

- Incluir perfis de usuário
- Editar perfis de usuário
- Excluir perfis de usuário

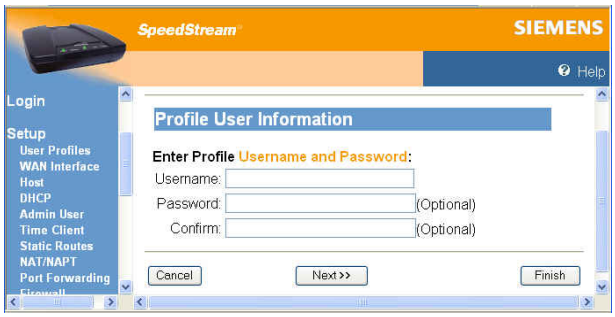
## Inclusão de perfis de usuário

Para incluir um novo perfil de usuário:

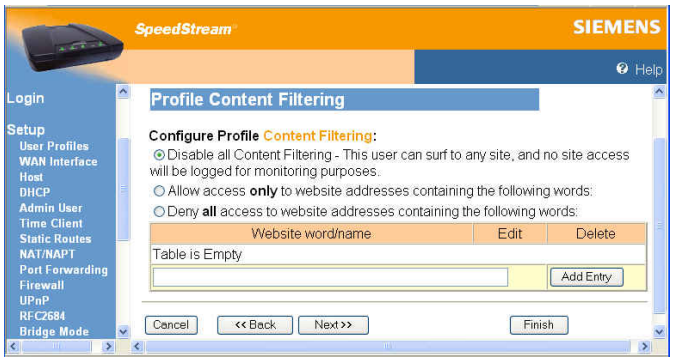
1. Selecione **Setup>User Profiles** (Configurar > Perfis de usuário) no painel de navegação à esquerda na interface da Web. A janela Current Profiles (Perfis atuais) é exibida. Os perfis de usuário são incluídos por meio do assistente, cujo acesso é feito desta janela.



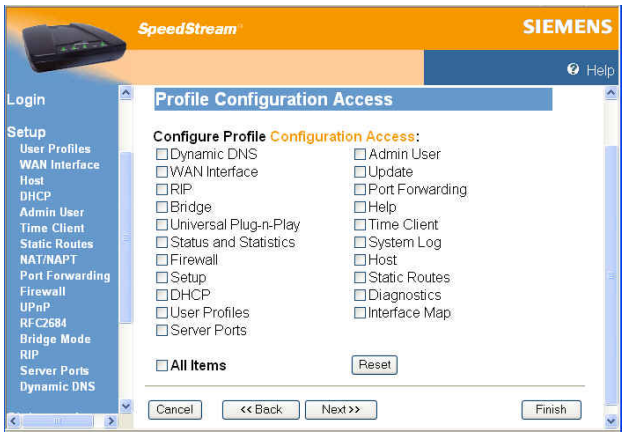

2. Opcionalmente, selecione a opção **Force all users to be identified before surfing** (Forçar todos os usuários a ser identificados antes de surfar).
3. Clique em **New Profile** (Novo perfil). A janela “Profile User Information” (Informações do perfil de usuário) é exibida.



4. Digite um nome de usuário para o usuário.
5. Opcionalmente, digite uma senha para o usuário e digite-a novamente no campo **Confirm** (Confirmar).
6. Clique em **Next** (Avançar). A janela “Profile User Filtering” (Filtragem do perfil de usuário) é exibida. A filtragem de conteúdo restringe o acesso a sites e conteúdo da Web indesejáveis.



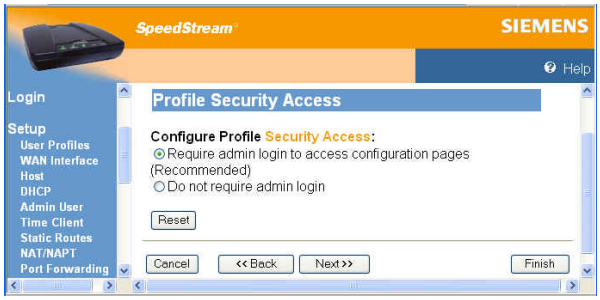

7. Selecione uma das opções de filtragem de conteúdo a seguir:
   - **Disable all Content Filtering** (Desativar toda a filtragem de conteúdo)
     O usuário tem acesso a todo conteúdo da Internet sem restrições.
   - **Allow access only to website addresses containing the following words** (Permitir acesso apenas a endereços de sites da Web que contenham as seguintes palavras)
     O usuário tem acesso apenas a determinados endereços de sites na Web ou a endereços que contenham entradas de palavra definida na tabela de palavra/nome de site da Web.
   - **Deny all access to website addresses containing the following words** (Negar todo o acesso a endereços de site que contenham as seguintes palavras)
     O usuário tem o acesso negado a todos os endereços de sites da Web especificados assim como a todos os endereços que contenham qualquer palavra definida na tabela de palavra/nome de site da Web.
8. Se a opção **Allow access only…**(Permitir acesso apenas...) ou **Deny all access**…(Negar todo acesso...) for selecionada, digite uma palavra ou endereço da Web na caixa abaixo da tabela de palavra/nome de site da Web e clique em **Add Entry** (Adicionar entrada). O sistema responde com a inclusão da palavra ou do endereço da Web na tabela de palavra/nome de site da Web. Isso pode ser feito diversas vezes para incluir diferentes entradas à tabela.
9. **Nota:** As entradas na tabela de palavra/nome de site da Web podem ser modificadas ou excluídas a qualquer momento ao clicar em **Edit** (Editar) ou **Delete** (Excluir) próximos à palavra ou endereço da Web correspondente.
10. Clique em **Next** (Avançar). A janela “Profile Configuration Access” (Acesso à configuração do perfil) é exibida. O acesso à configuração do perfil define a permissão de acesso de um usuário pelo controle das funções e recursos disponíveis para aquele usuário.




11. Opcionalmente execute uma das ações a seguir:

    - Clique em um ou mais dos recursos disponíveis de forma a permitir o acesso do usuário àquele(s) recursos(s). Um marca de seleção será colocada na caixa correspondente (clique novamente para remover a marca de seleção e negar o acesso).
    - Clique em **All Items** (Todos os itens) para selecionar todos os recursos da lista.
    - Clique em **Reset** (Redefinir) para desmarcar todos os itens selecionados e negar o acesso do usuário àqueles recursos.

12. Clique em **Next** (Avançar). A janela “Profile Security Access” (Acesso à segurança do perfil) é exibida.




13. Clique em uma das opções a seguir:

    - **Require admin login to access configuration pages** (Requer login de administrador para acessar as páginas de configuração)
      O usuário deve efetuar o login como administrador para alterar a configuração do roteador. Esta é configuração recomendada.
    - **Do not require admin login** (Não requer login de administrador)
      O usuário poderá alterar a configuração do roteador sem a necessidade de informar uma senha.

14. Clique em **Next** (Avançar). A janela “Constant Profile IP Address” (Endereço IP do perfil constante) é exibida.

15. Opcionalmente, digite um endereço IP permanente associado a este perfil.
16. Clique em **Next** (Avançar).
17. O assistente de perfil do usuário é concluído. Clique em **Finish** (Concluir) para fechar o assistente e voltar à janela de perfis atuais.

## Edição de perfis de usuário

Esta seção descreve como editar um usuário.

Para editar um usuário:

1. Selecione **Setup>User Profiles** (Configurar > Perfis de usuário) no painel de navegação à esquerda na interface da Web. A janela “Current Profiles” (Perfis atuais) é exibida.

2. Clique no nome do usuário que deseja alterar. A janela “Profile User Information” (Informações do perfil de usuário) é exibida. Faça as alterações desejadas.

3. Clique em **Next** (Avançar) para ir à janela seguinte a ser alterada. Faça as alterações desejadas.

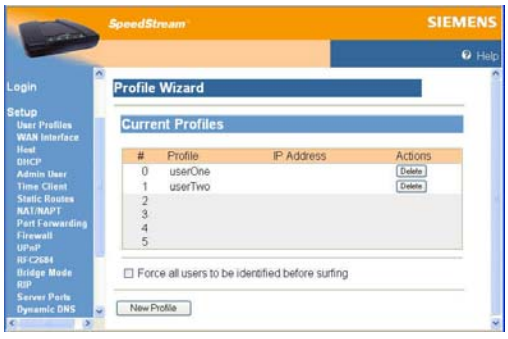
4. Clique em **Finish** (Concluir) a qualquer momento após concluir as alterações.

## Exclusão de perfis de usuário

Esta seção descreve como excluir um usuário.

Para excluir um usuário:

1. Selecione **Setup>User Profiles** (Configurar > Perfis de usuário) no painel de navegação à esquerda na interface da Web. A janela “Current Profiles” (Perfis atuais) é exibida.




2. Clique no botão **Delete** (Excluir) próximo ao nome do usuário que deseja excluir.

# Capítulo 6

# Configuração da conexão do provedor de serviço Internet

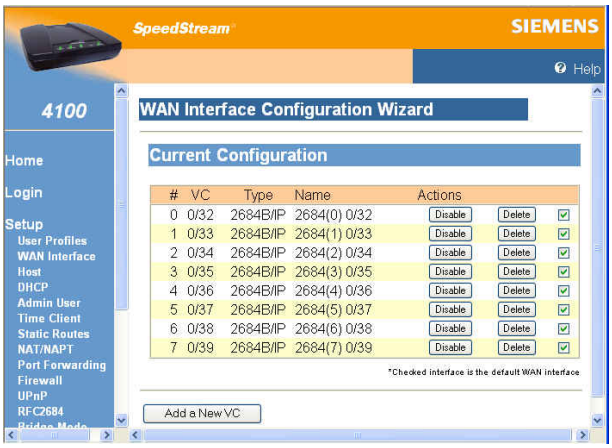
Este capítulo descreve como definir as configurações avançadas do provedor de serviço Internet. As opções nesta seção devem ser configuradas somente com orientação do seu provedor de serviços Internet. Alterações incorretas em qualquer uma das opções podem resultar em falhas de conexão com a Internet.

As opções de conexão do provedor de serviços de Internet estão listadas a seguir.

| | |
|---|---|
| Interface WAN | Assistente de configuração da interface WAN. As informações solicitadas pelo assistente devem ser fornecidas pelo provedor de serviço. |
| Host | Configura os atributos de básicos de rede do roteador (host). |
| DHCP | Configura e controla a funcionalidade do DHCP (protocolo de configuração de host dinâmico) e DNS. |
| Rotas estáticas | Adiciona e monitora rotas IP estáticas atribuídas pelo provedor de serviço Internet. A funcionalidade de roteamento do roteador aceita tanto roteamento dinâmico quanto roteamento estático. O roteamento estático se refere às rotas entre hosts conectados à rede que não são modificadas com o passar do tempo. |
| RFC2684 | Configura a funcionalidade DHCP na rede remota (WAN) para conexões baseadas em RFC2684. |

## Interface WAN

A conectividade à rede remota pode ser obtida por meio de um ou mais circuitos virtuais. Os circuitos virtuais são configurados por meio do assistente de configuração de interface WAN. As informações solicitadas pelo assistente devem ser fornecidas pelo provedor de serviço.

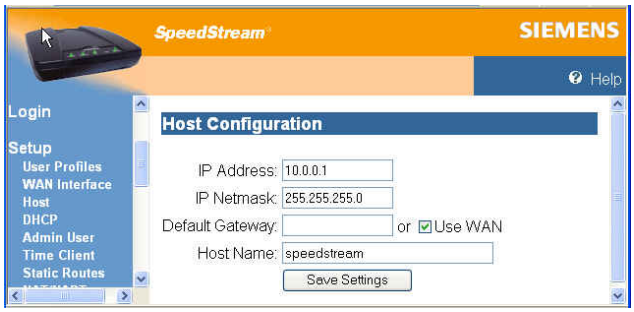


## Host

Os atributos de configuração do host identificam o roteador na rede e especificam opcionalmente um gateway padrão para a rede remota. Os valores padrão para muitos endereços IP de host, máscara de rede, roteador padrão e nome de host são gerados automaticamente para o roteador SpeedStream e não devem ser alterados, exceto quando determinado pelo provedor de serviço Internet. O provedor de serviço Internet pode solicitar que essas informações sejam modificadas se, por exemplo, um endereço IP estático for atribuído a você.

Para especificar as opções de configuração do host:

1. Selecione **Setup>Host** (Configurar > Host) no painel de navegação à esquerda na interface da Web. A janela “Host Configuration” (Configuração do host) é exibida.




2. Altere as configurações conforme orientação do seu provedor de serviços Internet.
3. Clique em **Save Settings** (Salvar configurações). Isso exibe uma tela de confirmação com a mensagem que a nova configuração só terá efeito após a reinicialização do roteador. Você pode reiniciar agora ou mais tarde.

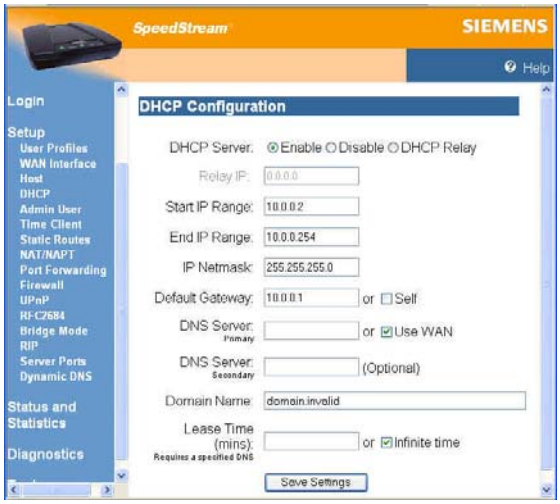
# DHCP

O protocolo de configuração de host dinâmico (DHCP) descreve os meios pelos quais um sistema pode conectar-se a uma rede para obter as informações necessárias para comunicação através dessa rede. Não modifique as opções de configuração padrão do DHCP, exceto quando determinado pelo provedor de serviço Internet.

**Nota:** Todos os endereços devem ser inseridos como uma máscara de sub-rede Ipv4 em formato decimal com ponto (por exemplo: 255.255.255.0).

Para configurar o recurso DHCP:

1. Selecione **Setup>DHCP** (Configurar > DHCP) no painel de navegação à esquerda na interface da Web. A janela “DHCP Configuration” (Configuração de DHCP) é exibida.




2. Selecione uma das opções a seguir:

   - **Enable** (Ativar)
     O roteador funcionará como um servidor DHCP para processar os pedidos DHCP recebidos dos hosts da rede local (clientes DHCP). O servidor DHCP não atende os clientes DHCP da rede remota.

     - **Ativar** é o modo de operação padrão do DHCP e o sistema gera automaticamente a faixa de endereço IP atual, máscara de rede IP e o roteador padrão.

     Não modifique as opções de configuração padrão, exceto quando determinado pelo provedor de serviço Internet.

   - **Disable** (Desativar)
     Desativa o DHCP. Se um endereço IP estático for utilizado, será necessário desativar o DHCP e digitar endereços diferentes nas caixas de texto.

   - **DHCP Relay** (Retransmissão DHCP)
     Ao invés de obter um endereço IP do roteador, o endereço IP é obtido do computador definido no campo de **Relay IP** (Retransmissão de IP). Utilizado quando as informações de DHCP forem recebidas de um servidor DHCP da rede remota. Os pedidos DHCP são encaminhados ao campo **Relay IP** da rede remota e as respostas DHCP são re-encaminhadas à rede local.

3. No campo **Start IP Range** (Interno IP inicial), digite o endereço IP inicial do intervalo de endereços com o qual o servidor DHCP atenderá os clientes com pedidos DHCP.

4. No campo **End IP Range** (Intervalo IP final), digite o endereço IP final do intervalo de endereços com o qual o servidor DHCP atenderá os clientes com pedidos DHCP.

   Essa definição de intervalo deve considerar as seguintes restrições de endereço:

   - O intervalo de endereços IP pode estender-se por apenas uma sub-rede IP.
   - O tamanho máximo do pool de endereços que pode ser gerenciado pelo servidor DHCP é igual a 64. Portanto, o intervalo de endereços não pode ser maior que 64.
   - O intervalo de endereços IP não deve incluir nenhum endereço IP mantido internamente pelo dispositivo SpeedStream para outros fins. Isso inclui o endereço IP estático do dispositivo da LAN, bem como o endereço IP padrão do roteador, endereços IP dos DNS primário e secundário e endereços IP de retransmissão primário e secundário.
   - Os intervalos de endereço IP numéricos para roteamento comumente usados são os seguintes:

     10.0.0.0 - 10.255.255.255
     172.16.0.0 - 172.31.255.255
     192.168.0.0 - 192.168.255.255

5. Em **IP Netmask** (Máscara de rede IP), digite a máscara de sub-rede IP que corresponde ao intervalo de endereços IP definido acima.
6. Em **Default Gateway** (Gateway padrão), execute uma das ações a seguir:
   - Digite o endereço IP de um gateway padrão ou roteador a ser fornecido para os clientes DHCP.
   - Clique em **Self** (Próprio) para especificar se o próprio roteador SpeedStream será usado como o gateway padrão.
7. Em **DNS Server (primary)** (Servidor DNS (primário), execute uma das ações a seguir:
   - Digite o endereço IP do servidor primário do sistema de nomes de domínio (DNS) a ser fornecido aos clientes DHCP. Um servidor DNS pode ser usado por clientes para resolver os nomes de domínio de endereços IP.
   - Clique em **Use WAN** (Usar WAN) para especificar que o endereço do servidor DNS fornecido pelo provedor Internet será fornecido aos clientes DHCP da rede local.
8. Em **Domain Name** (Nome de domínio), digite o nome de domínio DNS do servidor DHCP residente no dispositivo SpeedStream. O valor deve ser digitado como uma seqüência alfanumérica.
9. Em **Lease Time (**Tempo de concessão), execute uma das ações a seguir:
   - Digite o período de tempo em que um endereço IP concedido pelo servidor DHCP é válido. Ao final do período de concessão, o cliente DHCP transmitirá um pedido ao servidor para estender a concessão. O servidor estenderá o período de concessão do endereço IP atribuído ao cliente. Se o período de concessão expirar sem que o servidor receba um pedido de extensão da concessão do cliente, o servidor presumirá que a conexão do cliente não existe mais. O servidor liberará o endereço IP atribuído ao cliente e o devolverá ao pool de endereços disponíveis (se esta opção for selecionada, é preciso especificar um servidor DNS).
   - Clique em **Infinite Time** (Tempo indefinido):
     Deixa o tempo de concessão em aberto para evitar que o servidor libere o endereço IP.
10. Clique em **Save Settings** (Salvar configurações).

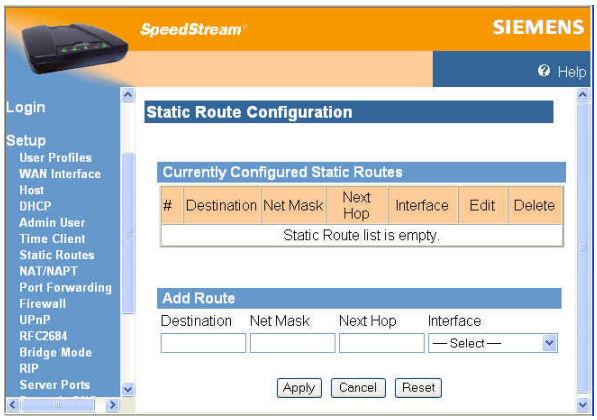
# Rotas estáticas

O roteador DSL SpeedStream controla o tráfego de dados “aprendendo” as informações de origem e destino e criando uma tabela de roteamento em seguida. Em alguns casos, mapeamentos de rede não podem ser conhecidos em função da incompatibilidade de esquemas de endereçamento. Algumas vezes pode ser desejável um caminho de origem e de destino diferente dos caminhos conhecidos, por exemplo, quando o provedor de serviço Internet atribui uma rota estática ao usuário. Nesse caso, as rotas estáticas podem ser configuradas para mapear um caminho desejado.

Use a opção avançada de rotas estáticas para configurar rotas estáticas até o equipamento remoto. O roteamento estático permite a definição de uma rota predefinida para a transmissão de dados. As rotas estáticas têm prioridade sobre todas as opções de roteamento dinâmico e oferecem maior segurança em relação ao roteamento dinâmico.

Para configurar uma rota estática:

1. Selecione **Setup>Static Routes** (Configurar > Rotas estáticas) no painel de navegação à esquerda na interface da Web. A janela “Static Route Configuration” (Configuração de rota estática) é exibida.




2. Em **Add Route** (Adicionar rota), digite o endereço IP do dispositivo de destino na caixa **Destination** (Destino).
3. Digite a máscara de rede do dispositivo de destino na caixa **Net Mask** (Máscara de rede).
4. Opcionalmente, digite o endereço IP para o qual os pacotes de dados serão encaminhados na caixa **Next Hop** (Próximo salto).
5. Selecione um tipo de conexão do menu **Interface**. A interface selecionada encaminhará os pacotes.
6. Clique em **Apply** (Aplicar). O sistema responde com a inclusão da sua nova rota à tabela de roteamento.
7. Este procedimento pode ser repetido para cada rota estática a ser incluída.

**Nota:** Para editar uma rota estática, clique na coluna **Edit** (Editar) da rota estática que deseja editar.

**Nota:** Para excluir uma rota estática, clique na coluna **Delete** (Excluir) da rota estática que deseja excluir.

# RFC2684

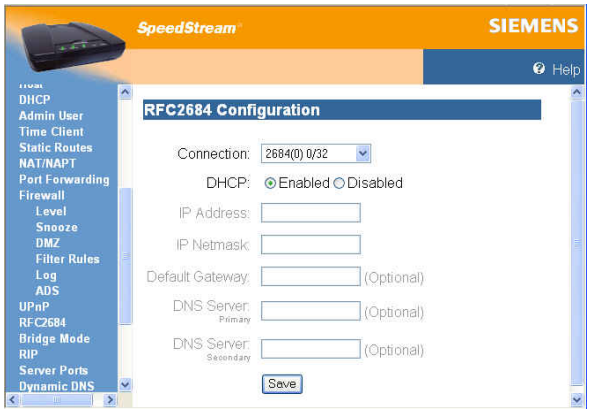
O roteador SpeedStream suporta dois tipos básicos de conexão: Ponto a ponto (PPP) e RFC2684.

Por padrão, as conexões RFC2684 dependem de um servidor localizado na rede remota (WAN) para fornecer ao roteador um endereço IP dinâmico e outros parâmetros de configuração baseados em IP à interface do roteador na rede remota (WAN). Isso é feito no roteador com a execução de um cliente DHCP (protocolo de configuração dinâmico do host) associado à conexão da rede remota. Esse cliente, por sua vez, comunica-se com o servidor DHCP localizado na rede remota.

Em alguns casos, esse procedimento automatizado pode não ser recomendável ou mesmo possível. Em tais situações, será preciso desativar o cliente DHCP no roteador e definir manualmente os parâmetros de configuração IP necessários fornecidos pelo provedor de serviços.

Para configurar a funcionalidade do RFC2684:

1. Selecione **Setup>RFC2684** (Configurar > RFC2684) no painel de navegação à esquerda na interface da Web. A janela “RFC2684 Configuration” (Configuração de RFC2684) é exibida.




2. Selecione a conexão que deseja configurar no menu **Connection** (Conexão).
3. Selecione uma das opções seguintes de **DHCP**:
   - **Enabled** (Ativo)
     Ativa o protocolo DHCP para a conexão selecionada.
   - **Disabled** (Inativo)
     Desativa o protocolo DHCP para a conexão selecionada.
4. Em **IP Address** (Endereço IP), digite o endereço IP a ser usado na interface WAN do roteador, normalmente obtido de um servidor DHCP na rede remota.
5. Em **IP Netmask** (Máscara de rede IP), digite a máscara de rede correspondente ao endereço IP.
6. Em **Default Gateway** (Gateway padrão) digite o endereço IP opcional de um roteador localizado na rede remota a ser usado como o gateway na rede remota.
7. Em **DNS Server** (Servidor DNS), digite o endereço IP opcional de um servidor DNS localizado na rede remota a ser usado para determinar nomes de domínio/endereços IP.
8. Clique em **Save** (Salvar).

# Capítulo 7

# Definição da configuração de rede

Esta seção contém detalhes das informações de configuração relacionada à rede. As opções de configuração da rede estão listadas abaixo:

| | |
|---|---|
| RIP | Ativa e controla a funcionalidade RIP. Com o uso do RIP, o roteador é capaz de determinar a menor distância entre dois pontos da rede com base nos endereços dos dispositivos de origem. |
| Redirecionamento de porta | Controla o acesso remoto a servidores LAN por meio de endereços IP privados. |
| UPnP | Configura e controla a interoperabilidade e segurança de UPnP. |
| Modo bridge | Configura o roteador como uma verdadeira ponte entre WAN e LAN. |
| Portas do servidor | Especifica as portas do servidor usadas por aplicativos comuns como HTTP (tráfego do site da Web), FTP e Telnet. |
| DNS Dinâmico | Configura DNS dinâmico. O DNS dinâmico converte os endereços IP em nomes alfanuméricos. Por exemplo: um endereço IP 333.136.249.80 pode ser convertido em siemens.com. |

## Protocolo RIP

Por padrão, o roteador SpeedStream não oferece suporte a protocolos de roteamento. No entanto, o suporte ao protocolo de informação de roteamento (RIP) versões 1, 2 ou 1 e 2 pode ser ativado. Esse suporte pode ser configurado para qualquer conexão de rede remota configurada atualmente ou para a rede local em geral.

Com o uso do RIP, o roteador é capaz de determinar a menor distância entre dois pontos da rede com base nos endereços dos dispositivos de origem. O RIP baseia-se em algoritmos de distância para calcular o menor caminho com o uso das informações na tabela de roteamento. O menor caminho baseia-se no número de saltos entre dois pontos.

Para usar a opção RIP:

1. Selecione **Setup>RIP** (Configurar > RIP) no painel de navegação à esquerda na interface da Web. A janela “RIP Configuration” (Configuração de RIP) é exibida.

2. Selecione uma das opções sob o cabeçalho **RIP Version** (Versão de RIP) próximo à conexão de sua escolha:

   **1**: Define a formatação de pacote RIP essencial para os pacotes de informações de roteamento.

   **2**: Define a formatação de pacote avançada para pacotes de informações de roteamento ao fornecer o seguinte: Endereço IP, máscara de sub-rede, próximo salto e métrica (mostra por quantos roteadores o pacote de roteamento passou até o seu destino).

   **1&2**: Uma combinação de ambos os tipos de pacotes RIP.

3. Selecione uma caixa de seleção **Active Mode** (Modo ativo) próxima à conexão correspondente para ativá-lo.

4. Clique em **Apply** (Aplicar). A janela “Your Settings Have Been Saved” (As configurações foram salvas) é exibida.

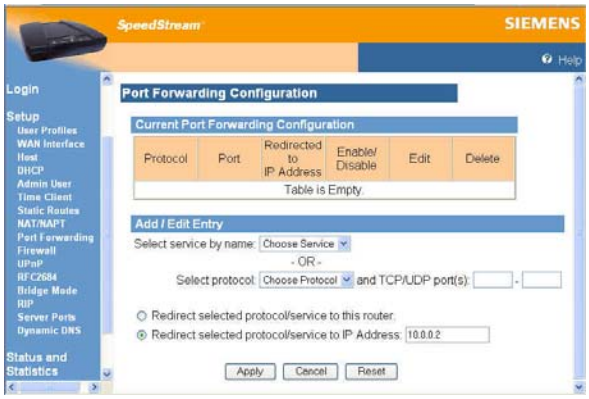
5. Opcionalmente, clique em **Reboot** (Reinicializar) se desejar que as configurações sejam implementadas imediatamente. O sistema responde com a reinicialização do seu roteador.

## Redirecionamento de porta

O redirecionamento de porta permite que os servidores localizados na rede local do roteador sejam acessados a partir da rede remota. Os pedidos de porta TCP ou UDP configurada provenientes da rede remota serão redirecionados ao endereço IP selecionado na rede local. A funcionalidade NAPT assegura que o servidor localizado na rede local seja conhecido na rede remota somente pelo endereço IP público. O endereço IP privado real do servidor permanece desconhecido a qualquer host na rede remota.

Para configurar o redirecionamento de porta:

1. Selecione **Setup>Port Forwarding** (Configurar > Redirecionamento de porta) no painel de navegação à esquerda na interface da Web. A janela “Port Forwarding Configuration” (Configuração de redirecionamento de porta) é exibida.




2. Em **Add/Edit Entry** (Adicionar/editar entrada), execute uma das ações a seguir:
   - Selecione o serviço que deseja configurar no menu **Select service by name** (Selecionar serviço pelo nome).
   - Selecione o protocolo que deseja configurar no menu **Select protocol** (Selecionar protocolo). As opções podem ser TCP, UDP, ICMP ou GRE. Se TCP ou UDP for selecionado, deve-se especificar também uma porta ou um intervalo de portas aplicáveis.
3. Selecione uma das opções a seguir:
   - Redirect selected protocol/service to this router (Redirecionar protocolo/serviço selecionado a este roteador)
     Selecione esta opção se desejar que o tráfego de entrada seja redirecionado ao SpeedStream.
   - Redirect selected protocol/service to IP address (Redirecionar protocolo/serviço selecionado para endereço IP)
     Selecione esta opção se desejar que o tráfego de entrada seja redirecionado a um host localizado na rede local. Neste caso, é preciso especificar o endereço IP do host no qual o servidor se encontra.
4. Clique em **Apply** (Aplicar).

## UPnP (Universal Plug and Play)

O Microsoft UPnP permite ao roteador comunicar-se diretamente com certos sistemas operacionais Windows para trocar informações sobre as necessidades especiais de certos aplicativos (como programas de trocas de mensagens ou jogos interativos), bem como fornecer informações sobre outros dispositivos da rede, quando aplicável. A comunicação entre o sistema operacional e o roteador reduz consideravelmente a quantidade de configuração manual exigida para o uso de novos aplicativos e dispositivos.

Apenas algumas versões do Windows XP e de computadores oferece suporte à função UPnP (Universal Plug and Play). Antes de configurar esta opção, assegure-se de que o componente UPnP esteja instalado e ativado em seu computador.

Para ativar a funcionalidade UPnP:

1. Selecione **Setup>UpnP** (Configurar > UpnP) no painel de navegação à esquerda na interface da Web. A janela “UPnP Configuration” (Configuração de UpnP) é exibida.

2. Selecione uma das opções de controle a seguir:

   - **Disable UpnP** (Desativar UpnP)
     Evita que o roteador use o recurso UPnP para comunicar-se com outros dispositivos ou com o sistema operacional. Pode ser desativado também se o sistema operacional não suportar UPnP.
   - **Enable Discovery and Advertisement only (SSDP)** (Ativar somente protocolo de serviço de descoberta (SSDP)
     Envia somente informações sobre novos dispositivos detectados (hardware). Nenhuma informação relativa a aplicativos ou serviços é transmitida.
   - **Enable full Internet Gateway Device (IGD) support** (Ativar suporte total a Internet Gateway Device (IGD)
     Permite ao roteador comunicar-se livremente com computadores na rede em relação a novos dispositivos, aplicativos e serviços se necessário para assegurar que estejam funcionando com a exigência mínima de configuração manual.

3. Selecione uma das opções a seguir:

   - **Enable access logging** (Ativar login de acesso)
     Gera uma mensagem de log do sistema sempre que um cliente UPnP acessar o roteador.
   - **Read-only mode** (Modo somente de leitura)
     Restringe o tipo de acesso que um cliente UPnP pode ter ao roteador. Apenas os pedidos no protocolo UPnP para consulta do status do roteador são permitidos. Quaisquer pedidos que possam modificar potencialmente o comportamento do roteador são bloqueados.

4. Clique em **Apply** (Aplicar) para aceitar as configurações. A janela “UPnP Finish” (Concluir UpnP) é exibida.

## Modo Bridge

O roteador aceita dois modos de operação básicos com relação à conectividade entre a rede local e a rede remota: modo bridge/roteamento e modo bridge.

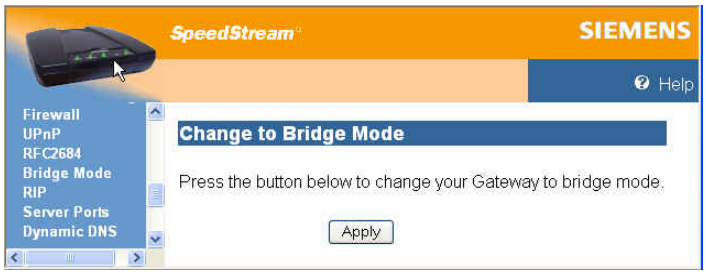
O modo bridge/roteamento é o modo de operação padrão. No modo bridge/roteamento, o roteador fornece a funcionalidade de roteamento normal entre a rede local (LAN) e a rede remota (WAN). No entanto, todas as interfaces da rede local são interligadas em ponte ("bridged").

O segundo modo de operação fornece apenas a funcionalidade de ligação em ponte. Isso se aplica tanto à conectividade WAN-LAN, bem como para todas as interfaces baseadas em LAN. As conexões ponto a ponto (PPP) não estão disponíveis no modo de operação “bridge”.

**Importante: S**e o modo bridge for selecionado, o acesso à interface da Web de gerenciamento será perdido e somente poderá retornar ao modo de roteamento recuperando-se as configurações originais de fábrica no roteador.

Para alternar ao modo bridge:

1. Selecione **Setup>Bridge Mode** (Configurar > Modo bridge) no painel de navegação à esquerda na interface da Web. A janela “Change to Bridge Mode” (Alterar para modo bridge) é exibida.



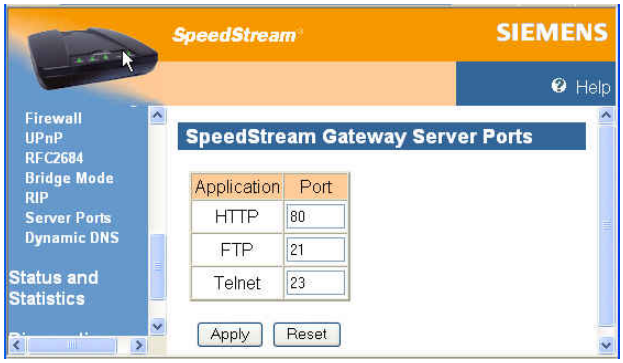

2. Clique em **Apply** (Aplicar).

## Portas do servidor

Aplicativos comuns como HTTP (tráfego de sites da Web), FTP e Telnet usam números de porta de entrada predefinidos para manter a compatibilidade com outros dispositivos. É possível alterar as portas usadas por esses aplicativos com o uso desta opção. Este recurso é recomendado apenas usuários avançados.

Para configurar a opção de porta do servidor:

1. Selecione **Setup>Server Ports** (Configurar > Portas do servidor) no painel de navegação à esquerda na interface da Web. A janela “SpeedStream Gateway Server Ports” (Portas de servidor do gateway SpeedStream) é exibida.




2. Opcionalmente, digite um número de porta na caixa **HTTP**. A porta padrão para este campo é 80.
3. Opcionalmente, digite um número de porta na caixa **FTP**. A porta padrão para este campo é 21.
4. Opcionalmente, digite um número de porta na caixa **Telnet**. A porta padrão para este campo é 23.
5. Clique em **Apply** (Aplicar). A janela “Your settings have been saved” (As configurações foram salvas) é exibida.
6. Opcionalmente, clique em **Reboot** (Reinicializar) se desejar que as configurações sejam implementadas imediatamente. O sistema responde com a reinicialização do seu roteador.

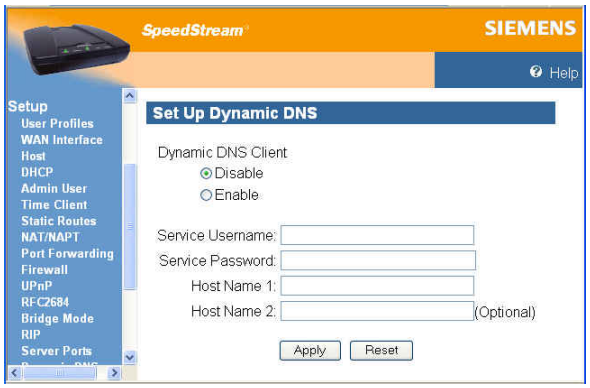
## DNS dinâmico

Use esta opção avançada para configurar o DNS dinâmico. O DNS dinâmico converte os endereços IP em nomes alfanuméricos. Por exemplo: um endereço IP 333.136.249.80 pode ser convertido em siemens.com. Para usar o serviço DDNS, o usuário deve registrar-se no serviço. O registro pode ser feita na página da Web a seguir: www.dydns.org/services/dydns.

Uma vez feito o registro, é necessário configurar os seus dados de DNS no roteador. Após registrar-se, os usuários podem conectar-se aos servidores (ou computador DMZ) via Internet utilizando o seu nome de domínio. Consulte a seção neste documento intitulada DMZ para obter mais informações sobre DMZ.

Para configurar o DNS dinâmico no roteador:

1. Selecione **Setup>Dynamic DNS** (Configurar > DNS dinâmico) no painel de navegação à esquerda na interface da Web. A janela “Set Up Dynamic DNS” (Configurar DNS dinâmico) é exibida.




2. Selecione a opção **Enable** (Ativar) em **Dynamic DNS Client** (Cliente DNS dinâmico).
3. Digite o nome fornecido a você por www.dydns.org na caixa **Service Username** (Nome de usuário do serviço).
4. Digite a sua senha de www.dydns.org na caixa **Password** (Senha).
5. Digite o nome de domínio ou de host fornecido por www.dydns.org na caixa **Host Name 1** (Nome do host 1).
6. Opcionalmente, se houver mais de um nome de domínio ou host, digite-o na caixa **Host Name 2** (Nome do host 2).
7. Clique em **Apply** (Aplicar). O sistema responde com o registro do seu nome de domínio ou de host em www.dydns.org.

# Capítulo 8

# Configuração dos recursos de segurança

O roteador oferece diversas medidas de segurança contra usuários indesejáveis. A segurança permite também a configuração do firewall, senha do administrador, conversão dos endereços de rede (NAT) e da “zona desmilitarizada” (DMZ). As opções de segurança estão listadas abaixo:

| | |
|---|---|
| Usuário admin | Gerencia o nome e a senha de login do administrador. |
| Time Client | Configura a funcionalidade de data e hora baseada na rede. Uma data e hora precisa devem ser usadas ao registrar eventos do sistema e do firewall, além de ser um requisito para algumas funcionalidades do firewall (por exemplo: operação de firewall compatível com ICSA). |
| NAT/NAPT | Configura e controla o endereçamento IP na rede local por meio de NAT ou NAPT. |
| Firewall | Configura e controla o firewall interno. Muitos desses recursos requerem uma compreensão profunda dos princípios de funcionamento das conexões em rede e operações de firewall. As opções do firewall estão listadas abaixo. |

## Usuário admin

O perfil do administrador controla os requisitos de acesso à interface da Web e às páginas de configuração, assim como a definição do nome e da senha de login do administrador.

Para definir as configurações do administrador:

1. Selecione **Setup>Admin User** (Configurar > Usuário admin) no painel de navegação à esquerda na interface da Web. A janela “Gateway Administrator Setup” (Configuração do administrador de gateway) é exibida.

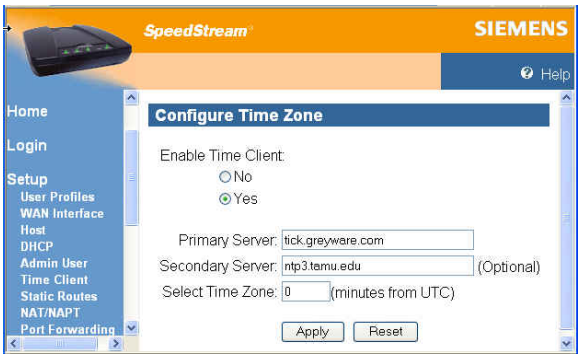
2. Especifique um nome de usuário para o administrador. Você pode aceitar o nome de usuário padrão **admin** ou digitar um novo nome de usuário em **User name** (Nome de usuário). O nome de usuário distingue entre maiúsculas e minúsculas.
3. Digite uma senha em **New Password** (Nova senha) e a mesma senha em **Confirm New Password** (Confirmar nova senha). O campo de senha distingue entre maiúsculas e minúsculas.
4. Selecione um nível de segurança de login dentre os relacionados a seguir:
   - **Require admin login to access entire Web site** (Requer login de administrador para ter acesso a todo o site da Web)
     Antes de ter acesso a qualquer tela na interface da Web, é necessário efetuar o login com o seu nome de usuário e senha na rede. (nível de segurança = alto)
   - **Require admin login to access configuration pages** (Requer login de administrador para ter acesso às paginas de configuração)
     Antes de acessar qualquer tela na interface da Web que permita alterar a configuração, é necessário efetuar o login com o seu nome de usuário e senha na rede. (nível de segurança = médio)
   - **Do not require admin login** (Não requer login de admin)
     Após efetuar o login pela primeira vez, não será mais necessário efetuar o login novamente em qualquer tela. (nível de segurança = baixo)
5. Clique em **Save Settings** (Salvar configurações).

# Time Client

Um registro de data/hora de log preciso é um dos requisitos dos definidos pelas recomendações do ICSA Labs para firewall (ver 3.0a). Para manter registros de data/hora precisos em cada mensagem de log, o firewall implementa um cliente SNTP (Simple Network Time Protocol). Isso permite que o sistema sincronize automaticamente a data e hora com o padrão de horário internacional UTC (Tempo Universal Coordenado). A data e a hora do sistema são definidas e corrigidas automaticamente através do(s) servidor(es) designado(s).

Para configurar o time client:

1. Selecione **Setup>Time Client** (Configurar > Time client) no painel de navegação à esquerda na interface da Web. A janela “Time Client Configuration” (Configuração do time client) é exibida.




2. Selecione **Enable** (Ativar) em **Enable Time Client** (Ativar time client).
3. Em **Primary Server IP Address** (Endereço IP de servidor primário), digite o endereço IP do servidor primário a ser usado como o servidor de horário (um servidor NPT (Network Time Protocol) conhecido).
4. Em **Secondary Server IP Address (**Endereço IP de servidor secundário), digite o endereço IP do servidor secundário a ser usado como o servidor de horário se o roteador não receber uma resposta do servidor primário.
5. Em **Select Time Zone** (Selecionar fuso horário), digite o fuso horário em minutos relativos ao UTC (Tempo Universal Coordenado).
6. Clique em **Apply** (Aplicar).

## Servidor NAT/NAPT

Os hosts individuais localizados em uma rede local são normalmente obrigados a usar endereços IP privados em lugar de endereços IP públicos. Os endereços IP privados, no entanto, não são conhecidos na rede pública (WAN). Para expor os endereços IP privados atribuídos à rede local à rede pública, o roteador pode ser configurado para utilizar uma de duas metodologias: conversão de endereços de rede (NAT) ou conversão de porta de endereço de rede (NAPT). O NAT pode expor à WAN um único host da LAN, ao passo que o NAPT pode expor múltiplos hosts da rede local. A funcionalidade NAT/NAPT pode ser configurada individualmente para cada conexão WAN.

Para configurar a funcionalidade NAP/NAPT:

1. Selecione **Setup>NAT/NAPT** (Configurar > NAP/NAPT) no painel de navegação à esquerda na interface da Web. A janela “NAT/NAPT Configuration” (Configuração de NAT/NAPT) com as conexões da interface WAN é exibida.

2. Selecione uma das opções a seguir para a conexão desejada:

   - **NAT & NAPT Disabled** (NAT e NAPT desativados)
     Desativa o NAT e o NAPT para configurar, por exemplo, rotas estáticas atribuídas pelo provedor de serviço Internet.
   - **NAT Only Enabled** (Apenas NAT ativado)
     Ativa o NAT e especifica o endereço IP de destino para os pacotes de entrada. Em algumas ocasiões o NAT é ativado como padrão, dependendo de sua configuração.
   - **NAPT Only Enabled** (Apenas NAPT ativado)
     Usa o NAPT apenas para processar endereços múltiplos com base nas regras de redirecionamento de porta.
   - **NAT&NAPT Enabled** (NAT e NAPT ativados)
     Alguns provedores de serviços suportam um NAT/NAPT simultâneo. Com essa configuração, uma única interface WAN pode aceitar diversas conexões NAT, sendo que cada conexão NAT pode, por sua vez, expor um único host da LAN através de um único endereço IP público da WAN. Por meio do NAT ou NAPT, o roteador garantirá que o host baseado na rede local seja conhecido na rede remota pelo endereço IP público da conexão WAN do roteador. O endereço IP privado atual do host permanece desconhecido a qualquer host ou servidor na rede remota.

3. Clique em **Apply** (Aplicar) após concluir a configuração de todas as conexões desejadas.

## Firewall

Um firewall é um sistema projetado para evitar o acesso não autorizado a ou de uma rede privada. O firewall foi projetado para proteger os hosts localizados na rede local contra ataques provenientes da rede remota. Não é fornecida proteção a ataques originados na rede local. Devido à natureza das operações do firewall e aos recursos de sistema necessários para manter as operações, o firewall pode afetar o desempenho do roteador, principalmente em situações de cargas elevadas de tráfego de rede.

O item de menu do firewall, acessível pelo painel de navegação à esquerda na interface da Web, se expande para fornecer uma lista de opções que podem ser ativadas ou desativadas. Há também links para configurar os detalhes mais complexos de cada recurso de segurança.

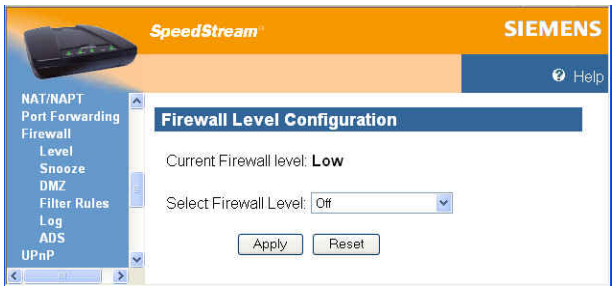
| | |
|---|---|
| Nível | Define o nível de segurança do firewall. |
| Intervalo de espera (snooze) | Desativa o firewall temporariamente. É importante observar que, quando o firewall estiver em estado de espera, toda a proteção fornecida pelo firewall estará desativada. |
| DMZ | Configura a DMZ do firewall para o controle de uma DMZ virtual na rede local. O objetivo da DMZ é redirecionar o tráfego de rede suspeito recebido de uma rede pública a um host seguro da rede local dedicado para essa finalidade. |
| Regras de filtragem | Inclui e exclui regras personalizadas para entrada e saída do firewall. |
| Log | Exibe um registro de atividades do firewall, incluindo registros de negação de acesso, códigos de motivos e descrições. |
| ADS | Configura os eventos contra os quais o sistema de detecção de ataques (ADS) interno fornecerá proteção e registro de uma lista de ataques conhecidos e provenientes da rede remota. |

## Nível

O firewall contido no roteador pode ser configurado para operar em um entre diversos modos, conhecidos como níveis. Para maior facilidade de uso, foram pré-configurados três níveis genéricos: baixo, médio e alto. Um nível distinto, compatível com a ICSA 3.0a, é fornecido para os usuários que necessitam de compatibilidade com os critérios definidos pelo ICSA Labs com relação ao comportamento do firewall (consulte o apêndice D, “Níveis de segurança do firewall”, no manual do usuário no CD-ROM para obter uma descrição detalhada dos três níveis pré-configurados).

Além dos níveis pré-configurados, há um nível personalizado para usuários avançados que exigem a opção de definir um conjunto personalizado único de regras para firewall. Para especificar o nível de segurança do firewall:

1. Selecione **Setup>Firewall>Level** (Configurar > Firewall > Nível) no painel de navegação à esquerda na interface da Web. A janela “Firewall Level Configuration” (Configuração de nível de firewall) é exibida.




2. Selecione uma das opções seguintes no menu **Select Firewall Level** (Selecionar nível de firewall):

   - **Off** (Desligado)
     Nenhuma restrição aplica-se ao tráfego de entrada ou de saída. Além disso, a funcionalidade NAPT é desativada. Uma vez que não há conversão de endereço/porta quando o firewall estiver operando nesse modo, todos os hosts conectados na rede local devem estar associados a um endereço IP público válido.

   - **Low** (Baixo)
     As restrições para o tráfego de saída são mínimas. O tráfego de saída é permitido para todos os aplicativos baseados em IP suportados e gateways de camada de aplicativo (ALGs). O único tráfego de entrada permitido é o recebido dentro do contexto de uma sessão de saída iniciada no host local.

   - **Medium** (Médio)
     As restrições ao tráfego de saída são moderadas. O tráfego de saída é permitido para a maioria dos aplicativos baseados em IP suportados e gateways de camada de aplicativo (ALGs). O único tráfego de entrada permitido é o recebido dentro do contexto de uma sessão de saída iniciada no host local.

   - **High** (Alto)
     Máxima restrição ao tráfego de saída. O tráfego de saída é permitido apenas para um conjunto bastante restrito de aplicativos baseados em IP suportados e gateways de camada de aplicativo (ALGs). O único tráfego de entrada permitido é o recebido dentro do contexto de uma sessão de saída iniciada no host local e autorizado por esse modo do firewall.

   - **ICSA 3.0a-compliant** (Compatível com ICSA 3.0a)
     Suporta os critérios do ICSA Labs definidos para o comportamento do firewall (para mais informações, visite o site da ICSA: http://www.icsalabs.com).

   - **Custom** (Personalizado)
     Permite a usuários avançados incluir, modificar e excluir suas próprias regras de firewall. Se esta

opção for selecionada, será preciso definir regras personalizadas para o tráfego de entrada e saída com o uso da opção de filtragem de IP.

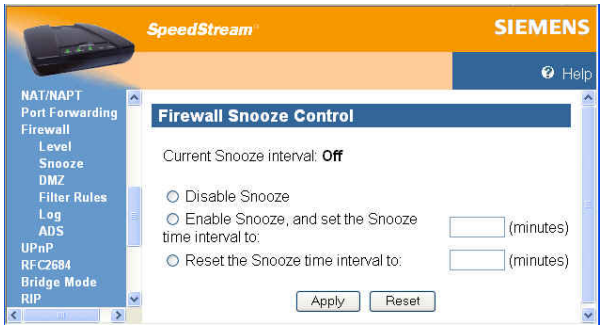
3. Clique em **Apply** (Aplicar).

## Intervalo de espera (snooze)

O recurso do intervalo de espera (snooze) permite desativar o firewall por um intervalo de tempo de forma que a equipe de suporte possa ter acesso a seu roteador ou rede ou para executar um aplicativo incompatível com o firewall. **Nota: Importante:** Esta função tem o seu uso recomendado apenas quando for necessário este nível especial de acesso irrestrito, uma vez que deixa o roteador e a rede sem a proteção do firewall.

Para ativar e configurar o controle do intervalo de espera:

1. Selecione **Setup>Firewall>Snooze** (Configurar > Firewall > Snooze) no painel de navegação à esquerda na interface da Web. A janela “Firewall Snooze Control” (Controle do intervalo de espera do firewall) é exibida.




2. Selecione uma das opções a seguir:

   - **Disable Snooze** (Desativar o intervalo de espera)
     Desativa todo o controle do intervalo de espera. Nesse modo, o firewall não está desativado.
   - **Enable Snooze, and set the Snooze time interval to** (Ativar intervalo de espera e definir o intervalo de tempo de espera em)
     Ativa o intervalo de espera por um determinado período de tempo. Certifique-se de digitar o valor em minutos para definir o tempo em que o firewall deve ficar desativado.
   - **Reset the Snooze time interval to** (Redefinir o intervalo de tempo de espera em)
     Reinicia o período de tempo do controle do intervalo de espera. Use esta opção se precisar uma extensão do tempo para uma sessão aberta de intervalo de espera. Certifique-se de especificar o período de tempo adicional (em minutos) em que o firewall deve ficar desativado.

3. Clique em **Apply** (Aplicar).

## DMZ

O firewall suporta DMZ virtual em modelos de roteador com uma única porta LAN.

A DMZ virtual redireciona o tráfego para um endereço IP determinado ao invés de uma porta física. Uma vez que esse redirecionamento é um aplicativo lógico em vez de físico, é chamado de DMZ virtual.

Com o uso da DMZ virtual, um único nó na rede local pode se tornar “visível” para a rede IP remota. Qualquer tráfego de rede de entrada não considerado pelas regras de redirecionamento de porta é automaticamente encaminhado a um nó de DMZ ativo. O tráfego de saída de um nó DMZ virtual não é bloqueado pelas regras de firewall. O recurso de DMZ permite a um computador na rede local contornar o firewall e ter acesso direto à Internet. Esse recurso é usado principalmente para jogos. Nesse modo de operação, todo o tráfego de rede recebido da rede pública que não seja destinado a um host especificamente exposto por meio de NAT ou a um servidor exposto por meio de redirecionamento de porta será redirecionado ao host DMZ designado. Se o recurso de DMZ for ativado, será preciso selecionar o computador a ser usado como o computador/host DMZ.

Esta função tem o seu uso recomendado apenas quando for necessário este nível especial de acesso irrestrito, uma vez que deixa o roteador e a rede sem a proteção do firewall. Para ativar e configurar o recurso DMZ:

1. Selecione **Setup>Firewall>DMZ** (Configurar > Firewall > DMZ) no painel de navegação à esquerda na interface da Web. A janela “Firewall DMZ Configuration” (Configuração da DMZ de firewall) é exibida.

2. Selecione uma das opções seguintes de ativação do recurso DMZ:

   - **Disable DMZ** (Desativar DMZ)
     O firewall não é neutralizado.
   - **Enable DMZ with this Host IP address** (Ativar DMZ com este endereço IP de host)
     O firewall é neutralizado através de um endereço IP digitado na caixa próxima a este campo.
   - **Enable DMZ with this Host IP address** (Ativar DMZ com este endereço IP de host)
     O firewall é neutralizado com um endereço IP selecionado no menu **Select Host** (Selecionar o host) próximo a este campo. Selecione o host desejado no menu suspenso.

3. Selecione uma das opções de fator de tempo a seguir:

   - **Make Settings Permanent** (Tornar as configurações permanentes)
     As configurações da DMZ são permanentes, exceto quando modificadas pelo administrador.
   - **Make Settings Last for** (Manter as configurações até)
     As configurações da DMZ são mantidas pelo período (em minutos) informado na caixa próxima a esta opção.

4. Clique em **Apply** (Aplicar).

## Regras de filtragem

Se o nível de segurança do firewall estiver definido como personalizado, este recurso permite especificar um conjunto exclusivo de regras de firewall para o tratamento do tráfego de entrada e de saída, que pode ser personalizado segundo os requisitos específicos do usuário. Nesse modo de operação, o firewall oferece um alto grau de configurabilidade. Desse modo, o recurso deve ser utilizado apenas por usuários avançados.

As regras podem ser baseadas na filtragem de qualquer um dos seguintes:

- Interfaces de roteador de origem e destino
- Protocolos IP
- Sentido do fluxo de tráfego
- Endereço IP da rede/host de origem e destino
- Atributos específicos do protocolo tais como tipos de mensagem ICMP
- Intervalos de porta de origem e de destino (para protocolos que os suportam) e suporte a operadores para comparação entre portas como menor que, maior que e igual a.

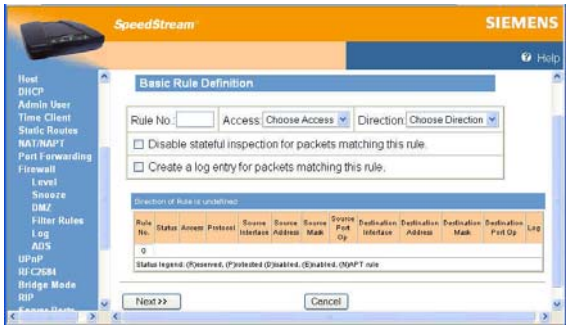
As regras podem permitir ou negar o fluxo de pacotes através do roteador de forma específica. Podem ser configuradas ações padrão a serem tomadas quando nenhuma regra específica for aplicável.

Para definir as regras de filtragem de IP de entrada e de saída:

1. Selecione **Setup>Firewall>Filter Rules** (Configurar > Firewall > Regras de filtragem) no painel de navegação à esquerda na interface da Web. A janela “Firewall IP Filter Configuration Wizard” (Assistente de configuração do filtro de IP do firewall) é exibida.

2. Execute uma das ações a seguir:
   - Para adicionar novas regras de filtragem de IP assim que forem definidas, clique em **Add New IP Filter Rule** (Adicionar nova regra de filtragem de IP). A janela “Definição de regra básica” será exibida.
   - Para clonar regras de filtragem de IP já definidas, clique em **Clone IP Filter Level** (Clonar nível de filtragem de IP).
   - A janela “Clonar regra de filtragem de IP” será exibida. Uma vez feita a clonagem, é possível modificar as regras existentes.

## Criação de regras personalizadas de filtragem de IP




Para adicionar uma nova regra:

1. Digite um valor numérico com até cinco dígitos na caixa **Rule No** (Nº da regra) para identificar exclusivamente a regra.
2. Selecione **Permit** (Autorizar) ou **Deny** (Negar) no menu **Access** (Acesso). Selecione **Permit** (Autorizar) para aceitar e **Deny** (Negar) para rejeitar a regra.
3. Selecione **Inbound** (Entrada) ou **Outbound** (Saída) no menu **Direction** (Sentido). **Inbound** refere-se aos dados recebidos no roteador, enquanto **Outbound** refere-se aos dados transmitidos do roteador.
4. Opcionalmente, selecione a opção **Disable stateful inspection for packets matching this rule** (Desativar inspeção minuciosa para pacotes que correspondem a essa regra) para evitar que o firewall crie uma sessão de inspeção minuciosa para os pacotes que correspondem a essa regra.
5. Opcionalmente, selecione a opção **Create a log entry for packets matching this rule** (Criar uma entrada de registro para pacotes que correspondem a essa regra). Quando selecionada, uma entrada é colocada no arquivo de registro quando os pacotes correspondem a essa regra.
6. Clique em **Next** (Avançar). A janela “Source & Destination Definition” (Definição de origem e destino) é exibida.

7. No cabeçalho **Source** (Origem), selecione uma conexão de rede do menu **Network Interface** (Interface de rede).
8. Selecione uma das opções a seguir:
   - **Any IP Address** (Qualquer endereço IP)
     Selecione esta opção se esta regra for aplicável a qualquer endereço IP de origem.
   - **This IP Address** (Este endereço IP)
     Selecione esta opção se uma regra for aplicável a um determinado endereço IP de origem.

9. Se a opção **This IP Address** (Este endereço IP) for selecionada, digite um endereço IP no campo **IP Address** (Endereço IP). Execute uma das ações a seguir:
   - Digite uma máscara de rede no campo **Netmask** (Máscara de rede).
   - Selecione **or Host** para usar a máscara de rede do seu roteador como a máscara de rede de origem.
10. No cabeçalho **Destination** (Destino), selecione uma conexão de rede do menu **Network Interface** (Interface de rede).
11. Selecione uma das opções a seguir:
    - **Any IP Address** (Qualquer endereço IP)
      Selecione esta opção se esta regra for aplicável a qualquer endereço IP de destino.
    - **This IP Address** (Este endereço IP)
      Selecione esta opção se uma regra for aplicável a um determinado endereço IP de destino.
12. Se a opção **This IP Address** (Este endereço IP) for selecionada, digite um endereço IP no campo **IP Address** (Endereço IP). Execute uma das ações a seguir:
    - Digite uma máscara de rede no campo **Netmask** (Máscara de rede).
    - Selecione **ou Host** para usar a máscara de rede do roteador como a máscara de rede de destino.
13. Clique em **Next** (Avançar). A janela “Protocol Definition” (Definição de protocolo) é exibida.

14. Execute uma das ações a seguir:
    - Selecione uma das opções de protocolo a seguir no menu **Select by Name** (Selecionar por nome). Isso define os tipos de pacotes filtrados.
      - **Any Protocol** (Qualquer protocolo)
      - **TCP (Transmission Control Protocol)**
        Proporciona um transporte de bytes confiável, seqüenciado e sem duplicação para usuários remotos ou locais. Clique em **Next** (Avançar) para exibir a janela “Opções de TCP/UDP”.
      - **UDP (User Datagram Protocol)**
        Proporciona a troca de datagramas sem confirmação e garantida de entrega. Clique em **Next** (Avançar) para exibir a janela “Opções de TCP/UDP”.
      - **ICMP (Internet Control Message Protocol)**
        Subsistema que proporciona a comunicação com uma estação. O aplicativo mais utilizado deste protocolo é o comando Ping. Clique em Next (Avançar) para exibir a janela “Opções de ICMP”.
      - **GRE** (Generic Routing Encapsulation):
        Um protocolo de encapsulamento usado principalmente para redes virtuais privadas (VPNs).

- Digite um número de protocolo no campo **Select by Number** (Selecionar por número).

15. Clique em **Finish** (Concluir).

## Janela de opções de TCP/UDP

A janela “Opções de TCP/UDP” será exibida se o protocolo TCP ou o UDP for selecionado na janela “Definição de protocolo”. Se um desses tipos de protocolo for selecionado, será preciso identificar as portas de origem e de destino.

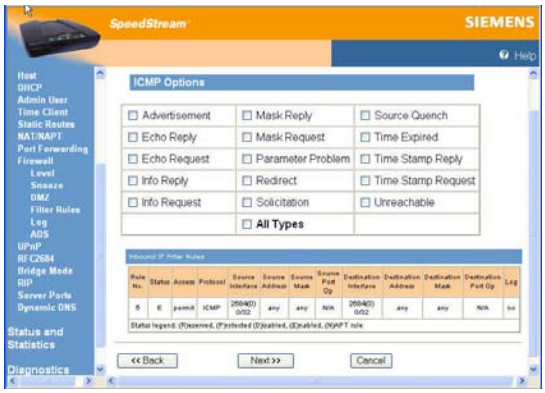
1. Selecione uma das opções a seguir no menu **Source Port Operator** (Operador de porta de origem) e no menu **Destination Port Operator** (Operador de porta de destino):

   - **any**
     Qualquer porta é aceitável como a porta de origem/destino.
   - **less than or equal to**
     Uma porta menor ou igual ao valor numérico no campo **Port 1** (Porta 1) é aceitável como a porta de origem/destino. Certifique-se de fornecer um valor no campo **Port 1**.
   - **equal to**
     Uma porta igual ao valor numérico no campo **Port 1** é aceitável como a porta de origem/destino. Certifique-se de fornecer um valor no campo **Port 1**.
   - **greater than or equal to**
     Uma porta maior ou igual ao valor numérico no campo **Port 1** é aceitável como a porta de origem/destino. Certifique-se de fornecer um valor no campo **Port 1**.
   - **range**
     Qualquer porta entre o valor numérico da entrada no campo **Port 1** e do valor no campo **Port 2** é aceitável como a porta de origem/destino. Certifique-se de fornecer um valor nos campos **Port 1** e **Port 2**.

2. Opcionalmente, marque a caixa de seleção **Check TCP syn packets** (Verificar pacotes de sincronização TCP) se desejar que esta regra evite o bloqueio dos pacotes de sincronização de sessões pré-existentes.
3. Clique em **Next** (Avançar).
4. Clique em **Finish** (Concluir).

## Janela de opções de ICMP

A janela “ICMP Options” (Opções de ICMP) será exibida se o protocolo ICMP for selecionado na janela “Definição de protocolo”.




1. Execute uma das ações a seguir:
   - Selecione qualquer uma das opções de ICMP que deseja filtrar.
   - Marque a caixa de seleção **All Types** (Todos os tipos) para filtrar todas as opções:
2. Clique em **Next** (Avançar).
3. Clique em **Finish** (Concluir).

## Clonagem de regras de filtragem de IP

A janela “Clone Rule Definitions” (Clonar definição de regra) será exibida quando a opção **Clone IP Filter Level** (Clonar nível de filtragem de IP) for selecionada na janela “Assistente de configuração do filtro de IP do firewall”. Com o uso desta opção, é possível clonar regras de nível alto ou baixo e modificá-las de acordo com as suas necessidades. Se a clonagem das regras de filtragem de IP for selecionada, as regras já definidas na tabela de Definição de regra serão descartadas.

Para clonar as regras de filtragem de IP:

1. Clique em **Clone IP Filter Level** (Clonar nível de filtragem de IP) da janela “Firewall IP Filter Configuration Wizard” (Assistente de configuração do filtro de IP do firewall). A janela “Clone Rule Definition” (Clonar definição de regra) é exibida.

2. Selecione uma das opções seguintes no menu **Select preconfigured firewall level for cloning** (Selecionar nível de firewall pré-configurado para clonagem).

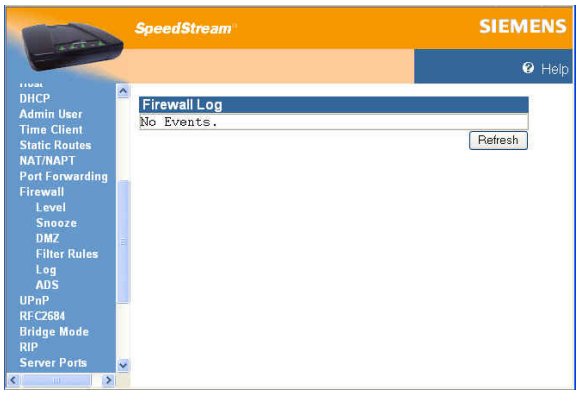
   - **Low** (Baixo)
     Clona as regras de nível baixo de filtragem de IP.
   - **Medium** (Médio)
     Clona as regras de nível médio de filtragem de IP.
   - **High** (Alto)
     Clona as regras de nível alto de filtragem de IP.

3. Clique em **Apply** (Aplicar). A janela “Assistente de configuração do filtro de IP do firewall” será exibida com o conjunto de regras selecionadas e mostradas na tabela Rule Definition (Definição de regra).
4. Desativa ou exclui qualquer regra.

# Registro (Log)

O registro de eventos (log) do firewall exibe as tentativas (bem e mal sucedidas) de acesso aos dados através do roteador. As entradas de registro do firewall estão definidas na tela **Firewall Settings Configuration** (Configurações do firewall) localizada no menu **Security** (Segurança).

Para visualizar as entradas de registro do firewall, selecione **Setup>Firewall>Log** (Configurar > Firewall > Log) no painel de navegação à esquerda na interface da Web. A janela “Firewall Log” (Log do firewall) é exibida.



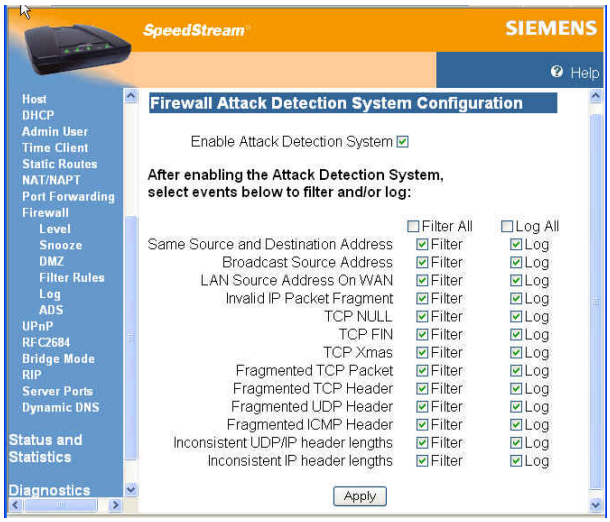
# ADS

O firewall fornece um avançado sistema de detecção de ataques (ADS) que pode ser utilizado para detectar e identificar diversos tipos de ataques originados na rede remota. O sistema possui a capacidade de detectar os ataques no momento em que são iniciados e proteger a rede local contra tais ataques.

Se o sistema de detecção de ataques for ativado, o roteador SpeedStream fornecerá proteção contra os ataques mais comuns de hackers que tentam acessar seu computador/rede pela Internet. As tentativas de invasão podem também ser gravadas no log para fornecer um registro das tentativas e de sua origem, quando disponível.

Para ativar e configurar o recurso de detecção de ataques:

1. Selecione **Setup>Firewall>ADS** (Configurar > Firewall > ADS) no painel de navegação à esquerda na interface da Web. A janela “Firewall Attack Detection System” (Sistema de detecção de ataques do firewall) será exibida.




2. Selecione **Enable Attack Detection** (Ativar detecção de ataques).
3. Marque a caixa de seleção **Filter** (Filtrar) de cada evento na lista que deseja filtrar ou, se desejar filtrar todos os eventos, marque a caixa de seleção **Filter All** (Filtrar todos). Isso proporciona a máxima proteção contra invasão maliciosa originada fora da rede.
4. Marque a caixa de seleção **Log** (Gravar no log) de cada evento na lista se desejar gravar no log ou marque a caixa de seleção **Log All** (Gravar todos no log) se desejar gravar todos os eventos. Quando o registro de eventos for selecionado para um determinado pacote malicioso, o ADS gravará uma entrada no log do firewall a cada minuto enquanto o ataque persistir. Isso mostra que um ataque de longa duração está ocorrendo sem preencher completamente o log do firewall com entradas para cada pacote separado.
5. Clique em **Apply** (Aplicar).

A seguir uma descrição de cada evento que pode ser monitorado.

- **Same Source and Destination Address** (Mesmo endereço de origem e de destino)
  Um dispositivo externo pode enviar um pacote de sincronização (SYN) para um host com os mesmos endereços de origem e de destino (inclusive da porta), causando o travamento do sistema. Ao tenta responder ao endereço de origem informado no pacote, o host receptor reenvia o pacote a si mesmo. O pacote pode continuar reverberando por mais de 200 vezes e consumindo recursos da CPU antes de ser descartado.

- **Broadcast Source Address (Broadcast para endereço de origem)**
  Um dispositivo externo pode enviar um teste de ping ao endereço de broadcast do roteador usando um endereço de origem falso. Quando o sistema responder aos testes de ping, será desativado pelas respostas de eco.
- **LAN Source Address on LAN** (Endereço de origem de LAN na LAN)
  Um dispositivo externo pode enviar um endereço de origem falso em um pacote IP de entrada para bloquear o rastreamento.
- **Invalid IP Packet Fragment** (Fragmento de pacote IP inválido)
  Um dispositivo externo pode enviar pacotes de dados fragmentados que podem desativar o seu sistema. Os pacotes de IP podem ser bastante grandes. Se um link entre dois hosts transportando um pacote processar apenas pacotes menores, o pacote maior poderá ser dividido ou fragmentado em pacotes menores. Ao atingirem o host de destino, os pacotes fragmentados devem ser remontados no pacote de tamanho maior como pedaços de um quebra-cabeça. Um fragmento inválido produzido de forma especial pode causar conflitos no host.
- **TCP NULL**
  Um dispositivo externo pode enviar um pacote IP com o campo de protocolo definido como TCP mas com um cabeçalho TCP e uma seção de dados nulos. Se o seu roteador responder a este ataque, o sistema será desativado.
- **TCP FIN**
  Um dispositivo externo pode enviar um ataque usando TCP FIN. Este ataque nunca permite que um pacote de dados finalize a transmissão e desativa o seu sistema.
- **TCP XMAS**
  Um dispositivo externo pode enviar um ataque usando pacotes TCP com todos os sinalizadores ativos. Isso pode tornar o sistema lento ou congestioná-lo.
- **Fragmented TCP Packet** (Pacote TCP fragmentado)
  Um dispositivo externo pode enviar um ataque usando pacotes fragmentados para permitir que um usuário Telnet externo possa ter acesso a um dispositivo em sua rede.
- **Fragmented TCP Header** (Cabeçalho TCP fragmentado)
  Um dispositivo externo pode enviar um ataque usando pacotes TCP com apenas um cabeçalho e sem nenhuma carga. Se vários ataques forem enviados através do roteador dessa maneira, o sistema ficará lento e poderá travar.
- **Fragmented UDP Header** (Cabeçalho UDP fragmentado)
  Um dispositivo externo pode enviar um ataque usando cabeçalhos UDP fragmentados para desativar um dispositivo em sua rede.
- **Fragmented ICMP Header** (Cabeçalho ICMP fragmentado)
  Um dispositivo externo pode enviar um ataque usando cabeçalhos ICMP fragmentados para desativar um dispositivo em sua rede.
- **Inconsistent UDP/IP header lengths** (Comprimentos de cabeçalho UDP/IP inconsistentes)
  Um dispositivo externo pode enviar um ataque usando cabeçalhos UDP/IP inconsistentes para desativar um dispositivo em sua rede.
- **Inconsistent IP header lengths** (Comprimentos de cabeçalho IP inconsistentes)
  Um dispositivo externo pode enviar um ataque usando alterações no cabeçalho IP para zerar o campo identificação de fragmento. Será tratado como um pacote completo quando for recebido e poderá congestionar o sistema.

# Capítulo 9

# Monitoramento do estado do roteador

*Este capítulo descreve como monitorar o estado do roteador.*

As opções listadas abaixo são usadas para avaliar o estado do roteador.

| | |
|---|---|
| Status e estatísticas | Exibe a Internet, rede local, estatísticas de segurança, arquivos de log do sistema e do firewall. |
| Diagnóstico | Executa um programa de diagnóstico de uma conexão selecionada em seu roteador. |
| Ferramentas | Redefine, reinicializa e atualiza o firmware. |

## Status e estatísticas

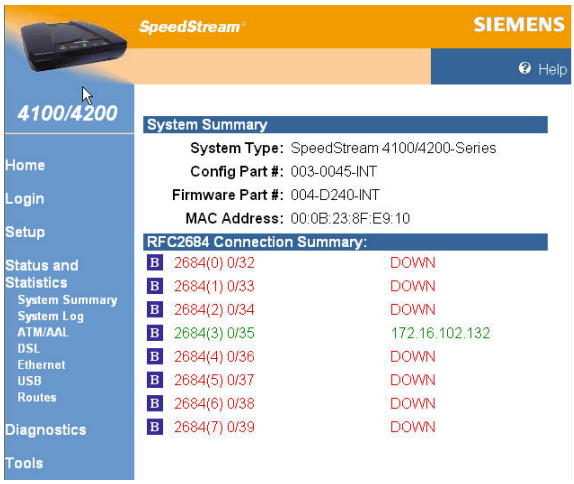
É possível exibir as estatísticas da Internet, rede local, segurança e do registro de eventos (log).

| | |
|---|---|
| Resumo do sistema | Informações descritivas básicas que identificam o roteador. |
| Log do sistema | Exibe um registro de toda atividade no sistema, incluindo as ações que foram executadas, pacotes ignorados e encaminhados. |
| ATM/AAL | Exibe as informações relativas ao status da conexão ATM. |
| DSL | Exibe as informações relativas ao status da conexão DSL. |
| Ethernet | Exibe as informações relativas ao status da conexão Ethernet. |
| USB | Exibe as informações relativas ao status da conexão USB. |
| Rotas | Exibe as informações relativas à tabela de roteamento atual. |

## Resumo do sistema

A janela “System Summary” (Resumo do sistema) fornece as descrições básicas que identificam o roteador, tipo de sistema, versões atuais de software e firmware, endereço MAC (identificador exclusivo de dispositivo) e status das conexões configuradas no momento.

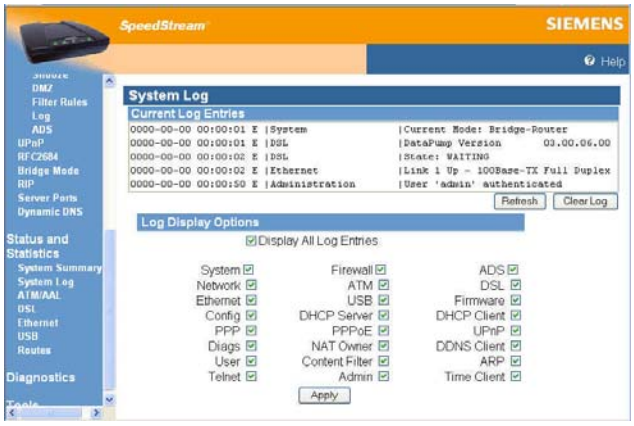
As informações de conexão incluem a identificação e o status atual das conexões ponto a ponto (PPP) e estáticas configuradas. Selecione **Status and Statistics>System Summary** (Status e estatísticas > Resumo do sistema) no painel de navegação à esquerda na interface da Web para visualizar estas informações.




## Log do sistema

A janela “System Log” (Log do sistema) exibe um registro de toda atividade no sistema, incluindo as ações que foram executadas, pacotes que foram ignorados e pacotes encaminhados. Essas informações permitem tomar decisões informando sobre a necessidade de adicionar novas regras de filtragem.

O log do sistema contém um máximo de 200 entradas e cada entrada pode conter um máximo de 200 caracteres. Selecione **Status and Statistics>System Log** (Status e estatísticas > Log do sistema) no painel de navegação à esquerda na interface da Web para visualizar a janela “Log do sistema”.

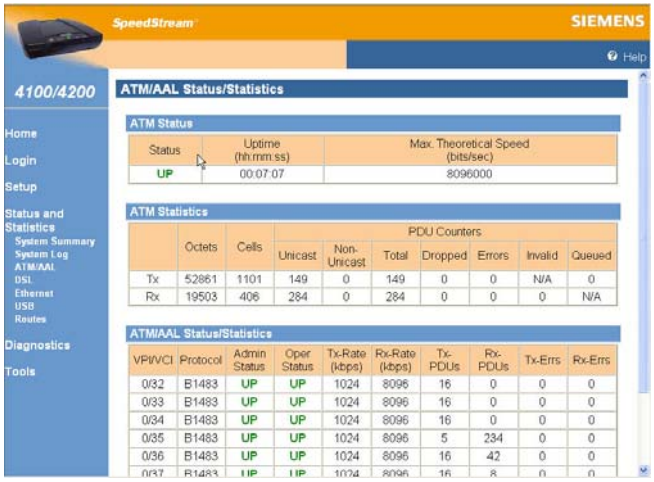



- Para atualizar a exibição, clique em **Refresh** (Atualizar).
- Para limpar o log, clique em **Clear Log** (Limpar log).

- Para alterar os eventos exibidos no log, modifique as **Log Display Options** (Opções de exibição do log) e clique em **Apply** (Aplicar).

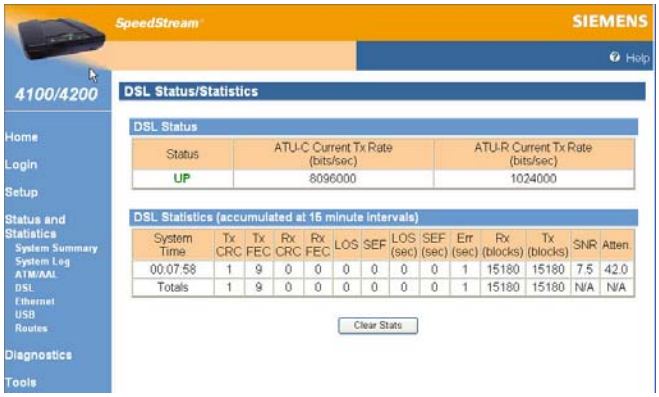
### Estatísticas de ATM

Exibe as informações de status e estatísticas de conexão com a rede ATM (Asynchronous Transfer Mode) na rede remota. A conexão remota com o provedor de serviços baseia-se em uma conexão de rede ATM. Além disso, são fornecidas informações estatísticas para cada circuito virtual configurado na camada ATM (AAL). Selecione **Status and Statistics>ATM/AAL** (Status e estatísticas > ATM/AAL) no painel de navegação à esquerda na interface da Web para visualizar as estatísticas de ATM/AAL. Esta janela exibe o status da conexão ATM, tempo de funcionamento, dados transmitidos/recebidos, VPI/VCIs e os dados correspondentes a cada circuito.




### Estatísticas de DSL

Exibe as informações de status e estatísticas da linha digital do assinante (DSL) quando a conexão de rede remota ao provedor de serviços for obtida por meio de uma linha DSL. As informações estatísticas são acumuladas a intervalos periódicos e podem ser exibidas para um período de até 24 horas. Selecione **Status and Statistics>DSL** (Status e estatísticas > DSL) no painel de navegação à esquerda na interface da Web para visualizar as estatísticas de DSL. Isso exibe as informações relativas à conexão DSL.

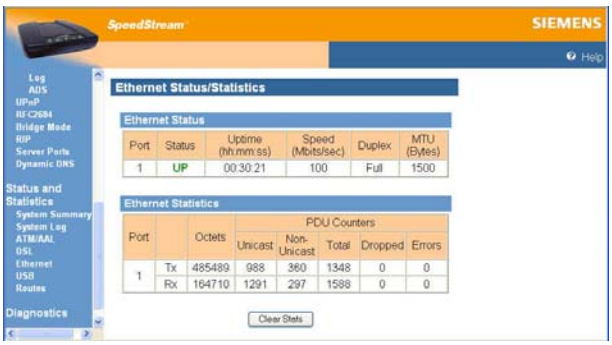


### Estatísticas de Ethernet

Exibe as informações de status e estatísticas de todas as conexões Ethernet da rede local.

Observe principalmente o status (“up” ou “down”) informado para cada porta Ethernet para confirmar se todos os cabos estão corretamente conectados e detectados pelo roteador.

Selecione **Status and Statistics>Ethernet** (Status e estatísticas > Ethernet) no painel de navegação à esquerda na interface da Web para visualizar as estatísticas de Ethernet.

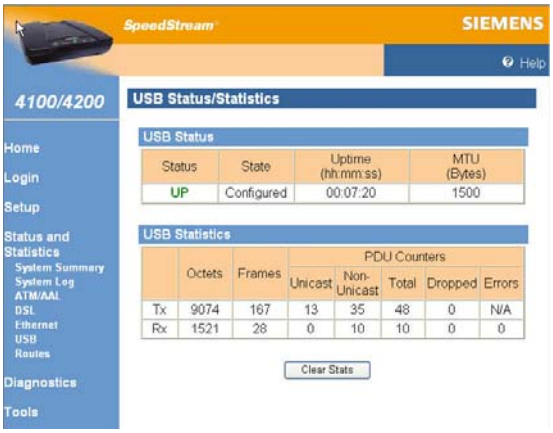



### Estatísticas de USB

Exibe as informações de status e estatísticas de todas as conexões USB da rede local.

Observe principalmente o status (ativo ou inativo) informado para cada porta USB para confirmar se os cabos estão corretamente conectados e detectados pelo roteador.

Selecione **Status and Statistics>USB** (Status e estatísticas > USB) no painel de navegação à esquerda na interface da Web para visualizar as estatísticas de USB.




### Rotas

Exibe todas as rotas IP conhecidas pelo roteador. Tanto as rotas estáticas como as dinâmicas são exibidas junto com a respectiva máscara de rede, roteador e a interface correspondente. Selecione **Status and Statistics>Routes** (Status e estatísticas > Rotas) no painel de navegação à esquerda na interface da Web para visualizar a tabela de roteamento atual, que contém os dados pertencentes a todas as rotas IP estáticas e dinâmicas conhecidas.

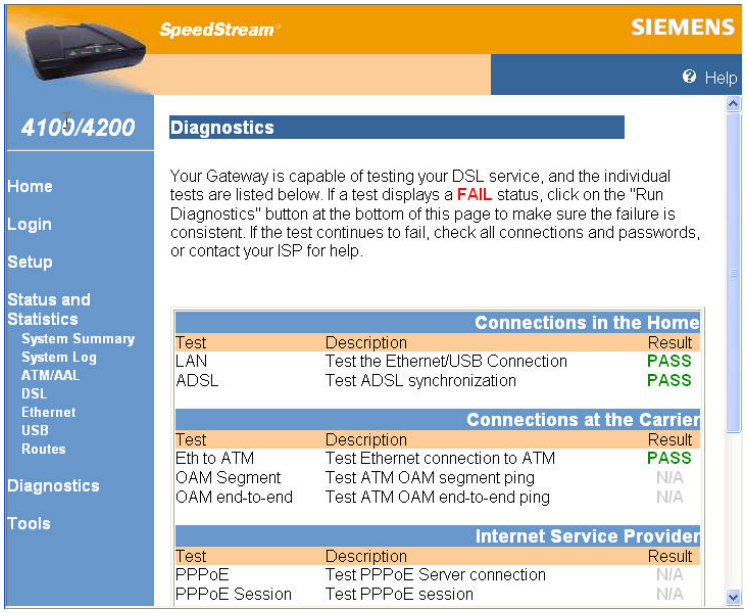
# Diagnóstico

O roteador fornece uma grande quantidade de recursos de diagnósticos para teste de conectividade tanto na rede local como na rede remota. Isso inclui conexões LAN na própria origem e conexões WAN para a operadora, provedor de serviço e Internet. O teste da rede remota pode ser executado para cada uma das conexões WAN configuradas. Os dados são normalmente solicitados pelo suporte técnico para ajudar na solução de problemas.

**Nota:** Esta opção pode não estar disponível na configuração de seu roteador.

Para executar o diagnóstico:

1. Selecione **Diagnostics** (Diagnóstico) no painel de navegação à esquerda na interface da Web. A janela “Diagnostics” (Diagnóstico) será exibida.


SpeedStream
SIEMENS
Help
4100/4200
Home
Login
Setup
Status and Statistics
System Summary
System Log
ATM/AAL
DSL
Ethernet
USB
Routes
Diagnostics
Tools
Diagnostics
Your Gateway is capable of testing your DSL service, and the individual tests are listed below. If a test displays a FAIL status, click on the "Run Diagnostics" button at the bottom of this page to make sure the failure is consistent. If the test continues to fail, check all connections and passwords, or contact your ISP for help.
Connections in the Home
Test Description Result
LAN Test the Ethernet/USB Connection PASS
ADSL Test ADSL synchronization PASS
Connections at the Carrier
Test Description Result
Eth to ATM Test Ethernet connection to ATM PASS
OAM Segment Test ATM OAM segment ping N/A
OAM end-to-end Test ATM OAM end-to-end ping N/A
Internet Service Provider
Test Description Result
PPPoE Test PPPoE Server connection N/A
PPPoE Session Test PPPoE session N/A

2. Selecione a conexão que deseja diagnosticar no menu **Connection to Test** (Conexão de teste).
3. Clique em **Run Diagnostics** (Executar diagnóstico). Os resultados do teste são exibidos na coluna **Results** (Resultados).

   Se um dos itens a seguir apresentar falha no diagnóstico, entre em contato com o seu provedor de serviços.

   - **Conexões na operadora**
   - **Provedor de serviço independente**
   - **Conectividade à Internet**
4. Se um teste exibir o status **FAIL** (falha) por qualquer outro motivo além dos mencionados acima, clique novamente em **Run Diagnostics** (Executar diagnóstico) para confirmar a falha.
5. Se o teste ainda exibir um status **FAIL**, verifique todas as conexões e senhas e clique novamente em **Run Diagnostics**.
6. Se o status de falha persistir, entre em contato com o seu provedor de serviços para obter mais assistência.

# Ferramentas

Esta seção descreve como usar as ferramentas listadas abaixo.

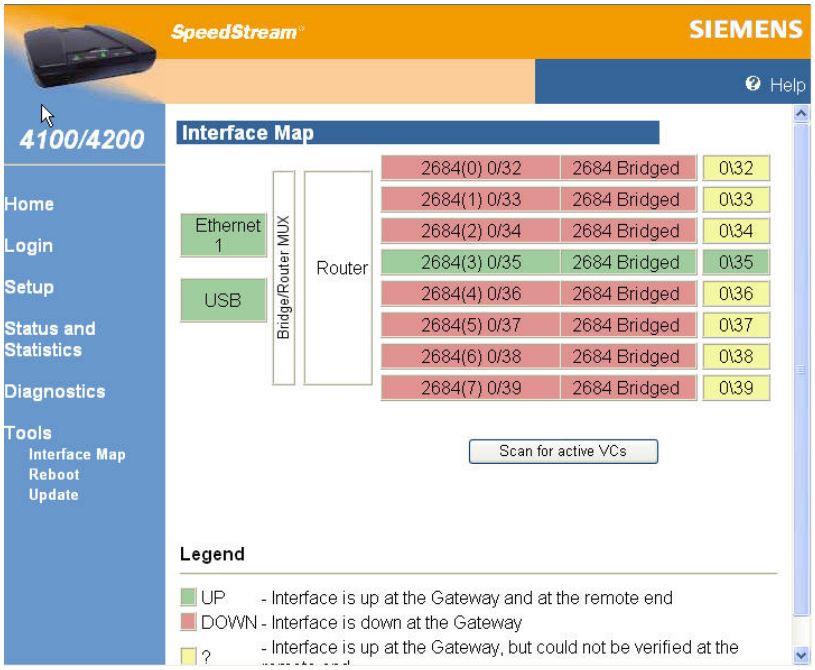
| | |
|---|---|
| Mapa de interface | Exibe uma representação gráfica das configurações atuais de LAN e WAN. |
| Reinicialização | Reinicializa o roteador |
| Atualização | Atualiza o firmware do roteador |

## Mapa de interface

Algumas configurações do roteador fornecem uma representação gráfica das configurações atuais da rede local e da rede remota. Essas informações são particularmente úteis para o suporte técnico, que poderá verificar se os encapsulamentos de protocolo corretos foram atribuídos e os circuitos virtuais estão mapeados para as interfaces de rede corretas.

**Nota:** Esta opção pode não estar disponível na configuração de seu roteador.

Para exibir o mapa de interface, selecione **Tools>Interface Map** (Ferramentas > Mapa de interface) no painel de navegação à esquerda na interface da Web. A janela “Interface Map” (Mapa de interface) será exibida.

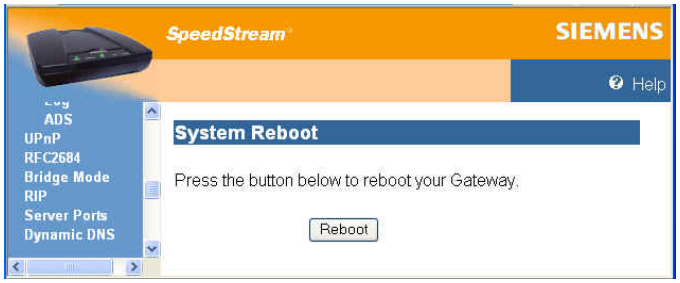


## Reinicialização

É possível reinicializar o roteador por meio da opção Reboot (Reinicializar) ou restaurar as configurações originais de fábrica no roteador por meio da opção Reset (Restaurar). A reinicialização deve ser usada quando o roteador precisa ser reiniciado sem perder as configurações atuais.

**Nota:** Esta opção pode não estar disponível na configuração de seu roteador.

Para reinicializar o roteador, selecione **Tools>Reboot** (Ferramentas > Reinicializar) no painel de navegação à esquerda na interface da Web. A janela “System Reboot” (Reinicialização do sistema) será exibida.




A janela “System Reboot” (Reinicialização do sistema) exibe uma contagem durante o processamento. Quando o roteador tiver reinicializado, será exibida a janela “System Summary” (Resumo do sistema).

### Restaurar os padrões do sistema:

A restauração dos padrões do sistema no roteador deve ser feita se for necessário recuperar as configurações originais de fábrica. Isso pode ser necessário quando uma configuração personalizada não produz os resultados esperados, quando se deseja uma nova configuração ou quando o roteador não parece estar funcionando corretamente. **Importante**: Esta opção redefine todas as configurações personalizadas, usuários e senhas em seu roteador.

**Nota:** Esta opção pode não estar disponível na configuração de seu roteador.

Para restaurar a configuração original do roteador:

1. Com o uso da ponta de uma caneta esferográfica ou um clipe de papel aberto, pressione e mantenha pressionado o botão **Reset** localizado na parte inferior do roteador. O LED **pwr** piscará uma vez na cor vermelha, indicando que a restauração teve início.
2. Continue pressionando o botão **Reset** por quatro segundos ou até que o indicador **PWR** comece a piscar alternadamente na cores vermelha e verde.
3. Solte o botão **Reset**.

### Para cancelar a restauração:

Continue pressionando o botão **Reset** por mais de 10 segundos. O LED **pwr** retornará ao verde e a ação será cancelada.

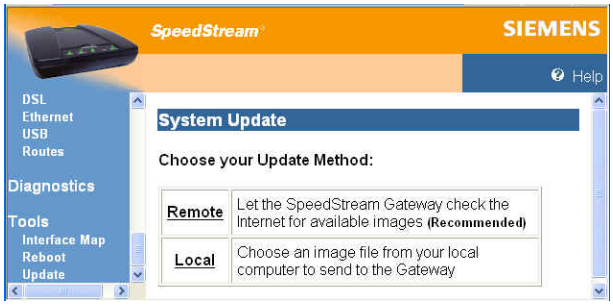
## Atualização

Esta opção atualiza o firmware do seu roteador pela Internet ou a partir de um dispositivo conectado ao seu roteador.

**Nota:** Esta opção pode não estar disponível na configuração de seu roteador.

Para atualizar o firmware:

1. Selecione **Tools>Update** (Ferramentas > Atualizar) no painel de navegação à esquerda na interface da Web. A janela “System Update” (Atualização do sistema) será exibida.




2. Selecione uma das opções a seguir:

   - **Remote** (Remota)
     Verifica na Internet a disponibilidade do arquivo de atualização adequado. Esta é o método recomendado.
   - **Local**
     Executa o download do arquivo de atualização do firmware de um local em sua rede. Antes de fazê-lo, será necessário fazer o download do arquivo de atualização para o computador.

**Importante**: Não desligue ou interrompa o roteador durante uma sessão de atualização do firmware. O roteador pode ficar inoperante.

# Apêndice A

# Solução de problemas

Os problemas de conexão normalmente ocorrem quando a configuração do software do roteador contém informações incompletas ou incorretas. As ferramentas de diagnóstico do roteador podem ajudar a identificar e resolver muitos desses problemas.

## Etapas para a solução de problemas básicos

Antes de contatar o suporte técnico, tente solucionar o problema seguindo as seguintes etapas:

1. Verifique os LEDs no painel frontal para diagnosticar o possível problema.
2. Verifique os problemas específicos tratados neste capítulo e siga as instruções para a sua solução.
3. Reinicialize o roteador. Todas as configurações feitas serão salvas.
4. Restaure o roteador apenas como um último recurso. Todas configurações feitas não serão salvas.

## Interpretação do mostrador de LED

Os LEDs indicadores no painel frontal do roteador fornecem um indício visual da atividade do roteador. Quando o roteador estiver configurado e funcionando corretamente, todos os indicadores LED rapidamente apresentam uma cor verde uniforme. A tabela a seguir mostra os estados possíveis indicados pelos LEDs. Se os LEDs indicarem um problema, consulte “Solução de problemas específicos” mais adiante neste capítulo.

| **LED** | **pwr** | **dsl** | **USB** | **enet*** |
|---|---|---|---|---|
| **Desligado** | Roteador sem alimentação | - Sem alimentação<br>- Sinal DSL não detectado | - Sem alimentação<br>- Nenhum dispositivo USB conectado<br>- Driver USB não instalado ou instalado incorretamente | - Sem alimentação<br>- Nenhum dispositivo Ethernet conectado<br>- Uso de cabo Ethernet incorreto (cross-over ao invés do de conexão direta) |
| **Verde** | Operação normal do sistema | Conectado e pronto para o tráfego de dados | Operação USB normal, link OK, sem tráfego do usuário | Operação Ethernet normal, link OK, sem tráfego do usuário |
| **Verde piscando** | N/D | - Piscando constantemente: DSL tentando conexão<br>- Piscando intermitentemente: DSL conectado e tráfego do usuário fluindo | Tráfego do usuário USB fluindo nos dois sentidos | Tráfego Ethernet do usuário fluindo nos dois sentidos |
| **Vermelho/ verde piscando** | “Flash write” em andamento | N/D | N/D | N/D |
| **Vermelho** | - Testes de POST em andamento (primeiros 30 segundos após ligar ou reinicializar)<br>- Ocorreu erro de POST | N/D | N/D | N/D |

# Solução de problemas específicos

#### LED *pwr* apagado

Se o indicador **pwr** estiver apagado, indica que o roteador não está conectado à fonte de alimentação. Verifique se o cabo de alimentação está conectado corretamente no painel traseiro do roteador e se a outra extremidade está ligada a uma tomada CA energizada.

#### LED *dsl* apagado

Se o indicador **dsl** estiver apagado, não há a detecção de um sinal válido da central telefônica. Verifique se o cabo DSL está conectado à porta correta do roteador e se o cabo de alimentação está ligado à tomada de energia elétrica. Se os cabos estiverem firmes, entre em contato com o seu provedor de serviços.

#### LED *enet* apagado

Isso indica que não há a detecção de um link Ethernet. Se o método de conexão via Ethernet for utilizado, verifique o cabo de conexão Ethernet do computador ao roteador. Se você estiver utilizando um cabo inadequado, o LED na placa de rede (NIC) do computador também estará apagado.

#### LED *USB* apagado

Isso indica que não há a detecção de um link USB. Se o método de instalação de USB for utilizado, verifique o cabo de conexão USB do computador ao roteador.

#### Erro de senha de login

Se após a solicitação da senha de login a mensagem de erro a seguir for exibida: **`Login Password is invalid:`**

- Digite a senha novamente e clique em **Save Settings** (Salvar configurações).
- Caso você tenha se esquecido da senha, será necessário restaurar o roteador.

**Nota:** A senha distingue entre maiúsculas e minúsculas. Verifique se a tecla Caps Lock foi ativada acidentalmente.

## Falha de POST (LED *pwr* vermelho)

POST (Power-on Self-test) realiza um autoteste no roteador. Ao ligar ou reinicializar o roteador, o indicador **pwr** apresenta um vermelho uniforme até que ocorra uma das duas situações a seguir: falha do teste POST inicial ou o teste é totalmente carregado e está pronto para ser executado.

- Se o POST passar sem falhas, o roteador prosseguirá até o final da inicialização e o indicador **pwr** se altera para verde uniforme.
- Se o teste de diagnóstico do POST inicial apresentar falha, o LED **pwr** permanecerá vermelho, indicando que ocorreu uma falha no POST e travará o roteador. Entre em contato com o suporte técnico da Efficient Networks para solucionar este problema.

## Contato com o suporte técnico

Caso o problema não tenha sido solucionado após os procedimentos recomendados de solução de problemas, entre em contato com o suporte técnico da Efficient Networks.

**Telefone:** (972) 852-1000

**Fax:** (972) 852-1001

**Email:** usa.800siemens@icn.siemens.com

**Internet:** http://www.icn.siemens.com/subscriber

# Apêndice B

# Níveis de segurança do firewall

A tabela a seguir mostra a segurança de cada modo do firewall para aplicativos e protocolos específicos.

**Nota:** Todos os aplicativos e protocolos têm permissão condicional IN (entrada) se a sessão tiver sido iniciada localmente e permissão OUT (saída).

| Aplicativo/Protocolo | Segurança (nível) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Alto | | Médio | | Baixo | | NAPT desativada | | Compatível c/m ICSA 3.0a. | |
| | In | Out | In | Out | In | Out | In | Out | In | Out |
| Abuse.Net | | | | √ | | √ | | √ | | |
| Age of Empires | | | | √ | | √ | | √ | | |
| AOL | | √ | | √ | | √ | | √ | | |
| AOL IM | | | | | | √ | | √ | | |
| Asherons Call | | | | √ | | √ | | √ | | |
| Baldur's Gate II | | | | √ | | √ | | √ | | |
| BattleNet | | | | √ | | √ | | √ | | |
| Buddy Telephone | | | | √ | | √ | | √ | | |
| Bungie.Net | | | | √ | | √ | | √ | | |
| Calista IP Telephone | | | | √ | | √ | | √ | | |
| Counterstrike | | | | √ | | √ | | √ | | |
| CUSeeMe | | | | | | √ | | √ | | |
| Delta Force | | | | √ | | √ | | √ | | |
| Descent II/III | | | | √ | | √ | | √ | | |
| Diablo | | | | √ | | √ | | √ | | |
| Diablo 2 | | | | √ | | √ | | √ | | |
| Dialpad | | | | √ | | √ | | √ | | |
| DirectPlay | | | | √ | | √ | | √ | | |
| DNS | | √ | | √ | | √ | | √ | | √ |
| Doom | | | | √ | | √ | | √ | | |
| Dune 2000 | | | | √ | | √ | | √ | | |
| EverQuest | | | | √ | | √ | | √ | | √ |
| FTP | | | | √ | | √ | | √ | | |
| GNUtella | | | | | | √ | | √ | | |

| Aplicativo/Protocolo | Segurança (nível) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Alto | | Médio | | Baixo | | NAPT desativada | | Compatível c/m ICSA 3.0a. | |
| | In | Out | In | Out | In | Out | In | Out | In | Out |
| H.323 | | | | | | √ | | √ | | |
| Half Life | | | | √ | | √ | | √ | | |
| Heretic II | | | | √ | | √ | | √ | | |
| Hexen II | | | | √ | | √ | | √ | | |
| HTTP | | √ | | √ | | √ | | √ | | √ |
| HTTPS | | √ | | √ | | √ | | √ | | √ |
| ICMP | | √ | | √ | | √ | | √ | | |
| ICQ 2000 | | | | | | √ | | √ | | |
| ICU II | | | | | | √ | | √ | | |
| IGMP | | | | √ | | √ | | √ | | |
| IPSec multi-session | | | | √ | | √ | | √ | | |
| IPSec single-session | | | | √ | | √ | | √ | | |
| IRC | | | | | | √ | | √ | | |
| Kali | | | | √ | | √ | | √ | | |
| L2TP | | | | √ | | √ | | √ | | |
| MechWarrior 4 | | | | √ | | √ | | √ | | |
| Mplayer | | | | √ | | √ | | √ | | |
| MS Netmeeting | | | | | | √ | | √ | | |
| MSN Gaming Zone | | | | √ | | √ | | √ | | |
| MSN Messenger | | | | | | √ | | √ | | |
| Myth | | | | √ | | √ | | √ | | |
| Napster | | | | | | √ | | √ | | |
| Need for Speed | | | | √ | | √ | | √ | | |
| Net2telephone | | | | √ | | √ | | √ | | |
| Netshow Client | | | | | | √ | | √ | | |
| NNTP | | | | | | √ | | √ | | |
| NTP | | | | √ | | √ | | √ | | √ |
| PCAnywhere | | | | | | √ | | √ | | |
| Ping | | √ | | √ | | √ | | √ | | |
| POP3 | | | | √ | | √ | | √ | | |

| Aplicativo/Protocolo | Segurança (nível) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Alto | | Médio | | Baixo | | NAPT desativada | | Compatível c/m ICSA 3.0a. | |
| | In | Out | In | Out | In | Out | In | Out | In | Out |
| PPPoE | | | | √ | | √ | | √ | | |
| PPTP multi-session | | | | √ | | √ | | √ | | |
| PPTP single-session | | | | √ | | √ | | √ | | |
| Quake Arena | | | | √ | | √ | | √ | | |
| Quake II | | | | √ | | √ | | √ | | |
| Quicktime 4 | | √ | | √ | | √ | | √ | | |
| Rainbow Six | | | | √ | | √ | | √ | | |
| Real Audio | | √ | | √ | | √ | | √ | | |
| Real Video | | √ | | √ | | √ | | √ | | |
| Red Alert II | | | | √ | | √ | | √ | | |
| Rogue Spear | | | | √ | | √ | | √ | | |
| RTSP | | √ | | √ | | √ | | √ | | |
| SIP | | | | | | √ | | √ | | √ |
| SMTP | | | | √ | | √ | | √ | | |
| Soldier of Fortune | | | | √ | | √ | | √ | | |
| SSH | | | | √ | | √ | | √ | | |
| Starcraft | | | | √ | | √ | | √ | | |
| T.120 | | | | | | √ | | √ | | |
| Telnet | | | | √ | | √ | | √ | | √ |
| Tiberian Sun | | | | √ | | √ | | √ | | |
| Traceroute | | √ | | √ | | √ | | √ | | |
| Ultima Online | | | | √ | | √ | | √ | | |
| Unreal Tournament | | | | √ | | √ | | √ | | |
| VNC | | | | | | √ | | √ | | |
| Warcraft | | | | √ | | √ | | √ | | |
| Windows Media Player | | √ | | √ | | √ | | √ | | |
| XDM | | | | | | √ | | √ | | |
| Yahoo Messenger | | | | | | √ | | √ | | |

**Siemens Subscriber Networks**
4849 Alpha Road
Dallas, TX 75244 EUA
Tel.: +1 (972) 852-1000
Fax: +1 (972) 852-1001
usa.800siemens@icn.siemens.com
http://www.icn.siemens.com/subscriber